Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 122 – 127

Procedia Computer Science

Building an Authentication and Quality of Query Services in the Cloud

J.Sunitha[a], Mrs. A.M.Sermakani[b]

[a]PG Student, S. A. Engineering College, Computer Science and Engineering, Chennai, India
Email: sunithaj04@gmail.com
[b]Assistant Professor, S. A. Engineering College, Information and Technology, Chennai, India
Email: sermakani@gmail.com

Abstract

Cloud outpouring is careful when an information distributor has given sensitive data to a set of trusted agents and few of the information is leaked and found in an unauthorized place. An enterprise data leak may be a scary proposition. Security practitioners always deal with data cloud leakage issues that arise from various ways like e-mail and different net channels. In case of information cloud leakage from trusted agents, the distributor should assess the probability that the leaked information came from one or more agents.

The proposed system can identify those parties who are guilty for such cloud leakage even once the data is altered. For this the system will use data allocation ways are also can inject "realistic but fake" information records improve the identification of cloud leakage. Moreover, data can also be leaked from inside an organization through e-mail. Hence there's also a need to filter these e-mails, may be done by blocking e-mails that contain pictures, videos or sensitive data in an organization. A principle utilized in e-mail filtering is classify e-mail based mostly the fingerprints of message bodies, the white and black lists of mail addresses and the words specified to spam.

Keywords: Sensitive data; Unauthorized access; E-mail filtering; Query privacy.

1. Introduction

Nowadays Peoples use cloud computing infrastructure because of its unique features in scalability and cost-saving. People use cloud because of its effective features such as security, infinite storage, low cost and multiple users can access the files applications in the cloud infrastructure. The owners in the cloud only pay for the time of using the server. This is an important feature because the workload of query services in the cloud is highly dynamic and it is dynamic. Even though the security is increased, the data confidentiality and query privacy are the major issue in cloud. The organization information's are also leaked through the e-mail within the organization.

To secure the data and query privacy new approaches are needed in the cloud. But it is not an advantage, if the new approaches for providing security and privacy will provide the slow query processing. The CPEL criteria are examined for submitting a query in the cloud. A CPEL criterion denotes confidentiality of data, query privacy, efficiency in query processing and low in-house working cost. This method increases the complexity of query services. Some related methods have been elaborated to identify some particular aspects of the problem. But they do not identify all these aspects. For example, the Order Preserving Encryption (OPE)[1] and crypto-index[8] methods are

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
doi:10.1016/j.procs.2015.04.073

vulnerable to the attacks. Enhanced crypto-index method[9] gives heavy load on the in-house infrastructure to improve the data security and query privacy. New Casper approach[13] uses cloaking boxes to secure data objects and query, which affects query processing efficiency and the in-house workload.

We study techniques for detecting leakage of a set of records. This paper develops a sample that can be estimated the "guilt" of agents. We also introduce algorithms for distribution of objects to agents that improves the chances of identifying leakier. This system also considers the method of adding fake objects to the distributed set. If it turns out an agent was given one or more fake objects that are leaking, then the distributor is more confident that the agent was guilty. The proposed system provides a method for calculating the guilt probabilities in case of information leakage. The next part provides a method for data allocation agents. Finally, evaluate the methods in different data leakage scenarios, and check whether they help to identify the leaker.

The proposed Random Space Perturbation (RASP) method is used to construct the practical range query and k-nearest-neighbor (kNN) query services in the cloud. The proposed system will satisfy all the four aspects of CPEL criteria. RASP method also transforms the multidimensional data with the combination of order preserving encryption, random noise injection and random projection. The RASP approach and its combination provide the data confidentiality and protect the multidimensional range of queries and efficiently processing the query with indexing. The range query is used to retrieve the stored data from the database. It uses the upper and lower bounds to retrieve the data. K-nearest-neighbor query is to find the nearest record to the query point.

The proposed system also uses the e-mail filtering method to filter the mail that sends to the unauthorized user. The main aim of this proposed work is to identify the guilty agents.

1.1 Organization

This paper has organized into VI sections. Section II gives literature review of the work done related to data security. Section III describes about the proposed system. Section IV defines the algorithm used in the proposed system. Section V gives the architecture of the proposed method. Finally, section VI gives a conclusion of the work.

2. Related work

The following related works are referred for preparing proposed work.

2.1 Order Preserving Encryption

OPE represents Order Preserving Encryption is used for data that allows any comparison. And that comparison will be applied to the encrypted data; this will be done without decryption. It allows database indexes to be built over an encrypted table. The main drawback of this technique is the encryption key is too large and the implementation takes more time and space.

2.2 *Crypto-index method*

Crypto index method is vulnerable to attacks, but the working system of the crypto index has many difficult processes to provide the secured encryption and security and the New Casper approach is used to protect data and query but the efficiency of the query process will be affected.

2.3 Distance recoverable encryption

This method used for preserving the relationship between the nearest neighbors. Many attacks can be applied because the distances are exactly preserved[17, 10, 5.] Wong et al.[17] suggest that dot products are preserved instead of distances to find k- nearest neighbor which is more resilient to distance-targeted attacks. The drawback of DRE is, in