Volume : 4 | Issue : 4 | April 2015 • ISSN No 2277 - 8179

Research Paper

Constructing Secure and Effective Query Services in Cloud Using ACDD Method

Engineering

KEYWORDS : sensitive data; query privacy; e-mail filtering; unauthorized access

J.Sunitha — Anna University, S.A Engineering College, Department of Computer Science and Engineering

Mrs.A.M.Sermakani — Anna University, S.A Engineering College, Department of Information Technology

ABSTRACT

Cloud computing is the set of computing services over the internet on leased basis. Cloud services allow individuals and businesses to access their service from anywhere over internet. When the distributor sends the information to the set of trusted agents, few of the information is leaked. The enterprise data leakage lead the company into unprotected. These data leakage destroys the customer trust and damages the reputation. 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.It also uses the skip merge algorithm to protect the sensitive data from unauthorized access.

INTRODUCTION

Nowadays company uses cloud computing to store their information. The company also accesses the information and service from cloud based on their desires. Cloud computing is the payper-use based on their demand. IT resources can easily share through the internet. Lack of security is the major concern in cloud computing. Once the confidential information such as design specification, price list and clients details are leaked it lead the company into unprotected. This data leakage puts production in a weak position. When someone sells this information for profit it damages the company's reputation and trademark and destroys customer trust.

The proposed system implements the method to identify the information leaker and to protect the sensitive data. For this the system allocates the fake objects to improve the identification of leaker. The distributor will intelligently give the data to the agent in order to increase the chances of identifying the guilty agent by adding the fake (noise) objects into

the dataset. It also uses the skip merge algorithm to secure the information. This skip merge algorithm is used to filter the mail content that sends to the unauthorized client or agent.

The proposed Arbitrary Capacity Data Disturbance (ACDD) technique is used to construct the range query and N-Adjacent Community (NAC) query services in the cloud. The proposed system provides the confidentiality, privacy and efficiency. Range query is to recover the information from the database. N-Adjacent Community is to find out the nearest community to the user query point.

CASE STUDY

PROPOSED SYSTEM

Clients are registering in cloud with their personal information to get authentication. Here the nodes are added with their IP and MAC address. Authorized clients only can access the information from the cloud. Server maintains the log of all query processed. ACDD implementation will be controlled in this section. Detected Clone Node logs are maintained in this section. It is done by the administrator. Every authorized client should have an individual IP address and MAC address. This specific address is used to identify the clone node detection.

The server node will send some fake object in addition to the original data. This fake object is created based on the agent request. The clone node will be unaware of these fake data. Only the owner of the node knows where and how many fake objects inserted into the original data. There are two techniques used in fake object creation.

In E-Random implementation the agent receives the entire data object that satisfies the condition of the agents' data request. If the explicit data request with fake allowed, then the data distributor cannot modify or remove the requests from the agents. However distributor can insert the fake object. The e-optimal algorithm reduces each term of the objective summary by adding the maximum number of fake data to every set giving optimal solution.

In S-Random implementation the extra data object the agents request in total, the more recipients on average an object has; and the more objects are used among different agents, the more difficult it is to discover a guilty agent. In this algorithm, the agent receives only the subset of data object that can be given to the agent. The working of the Sample Data Request algorithm is same as the working of Explicit Data Request.

Private Information Retrieval (PIR) tries to keep the privacy of the data access pattern, while the information may not be encrypted. This PIR scheme is normally very costly. The efficiency side PIR, uses a pyramid hash index to perform efficiently in privacy preserving data-block execution based on the conception of Oblivious RAM. It is different from the setting of high throughput, range query processing. It addresses the query privacy issues and requires the authorized query users, the owner of the data, and the cloud to the collaborative process kNN queries. However, most computing operations are performed in the user's local system with strong interaction with the cloud server. The cloud server only gives query processing, which does not meet the fundamental of moving computing to the cloud.

Authorized client or agent only can distribute the data. While distributing the data the agent send the request to add the fake object. A data distributor has given sensitive data to the set of supposedly trusted agents. Some of the data are leaked and found in an unauthorized place. The distributor must assess the probability that the leaked data came from one or more agents, as opposed to having been separately gathered by other means.

Clone node is detected once the client sent the data to the unauthorized person. The clone node is not aware about the fake objects created by the server.

The skip merge algorithm is used to filter the email. Skip merge algorithm filter the mail content when the distributor send the information to unauthorized client. This process involves 6 steps.

Volume : 4 | Issue : 4 | April 2015 • ISSN No 2277 - 8179

- Identify the data.
- Remove stopping words such as this, is, a, etc.
- Remove or change the synonyms.
- Determine the priority of the word depending upon the sensitivity of the data.
- Compare data with predefined company datasets.
- Filter the data if it has company's important data sets.

SYSTEM ARCHITECTURE

The design phase provides the clear view about how the proposed system provides confidentiality and security of the data. It also describes how the system is to filter the sensitive data from the unauthorized user. This phase helps the user easily to understand about the project.

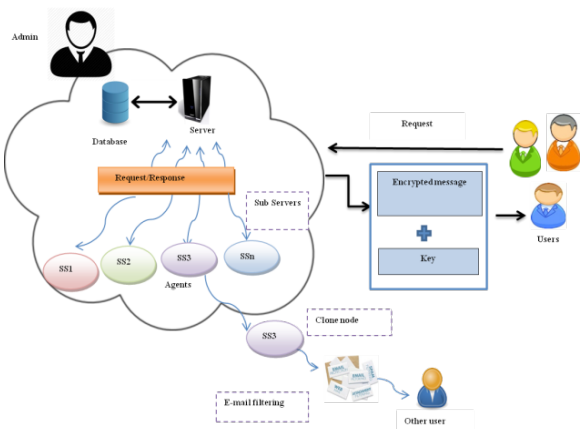

Fig. 1 *The System Architecture*

Fig. 1 describes the structure of the proposed system. The server will maintain all the login of the system. The clients and sub servers are registered in the cloud to get the authorization to access the cloud information. During the registration the server added the IP and MAC address of the user. These addresses are used to detect the clone node. The users or sub servers send the request to server to access the cloud information. After getting the request the server verify the database whether the users or sub server are the authorized party or not. The server creates the fake objects based on the sub server request. And then the server sends the encrypted message and key to the user. Only authorized user can able to transfer the data.

Once the clone node is detected, the skip merge algorithm is used to filter the e-mail from the clone node. The admin can view all the data transformation and admin get the e-mail alerts.

CONCLUSIONS

The proposed ACDD approach provides the confidentiality, efficiency of query processing and the privacy of query. This method also identifies which part of intermediate data sets need to be encrypted in order to save the privacy preserving cost. It also reduces the privacy preserving cost comparison with existing approaches. ACDD is the combination of encryption, random projection and noise injection, which provides the security feature. The proposed approach increases the detection of cloud leakage and provides the security to the cloud sensitive data. The skip merge algorithm is to secure the sensitive data from unauthorized access.

REFERENCE

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in INFOCOMM, 2011. | [2] K. Chen, R. Kavuluru, and S. Guo, "Rasp: Efficient multidimensional range query on attack-resilient encrypted databases," in ACM-Conference on Data and Application Security and Privacy, 2011, pp. 249–260. | [3] K. Chen and L. Liu, "Geometric data perturbation for outsourced data mining," Knowledge and Information Systems, 2011. | [4] K. Chen, L. Liu, and G. Sun, "Towards attack-resilient geometric data perturbation," in SIAM Data Mining Conference, 2007. | [5] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," ACM Computer Survey, vol. 45, no. 6, pp. 965–981, 1998. | [6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2006, pp. 79–88. | [7] H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, "Executing sql over encrypted data in the database-service-provider model," in Proceedingsof ACM SIGMOD Conference, 2002. | [8] B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in Proceedings of Very Large Databases Conference(VLDB), 2004. | [9] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in Proceedings ofACM SIGMOD Conference, 2006. | [10] K. Liu, C. Giannella, and H. Kargupta, "An attacker 's view of distance preserving maps for privacy preserving data mining," in Proceedings of PKDD, Berlin, Germany, September 2006. | [11] R. Marimont and M. Shapiro, "Nearest neighbour searches and the curse of dimensionality," Journal of the Institute of Mathematics and itsApplications, vol. 24, pp. 59–70, 1979. | [12] M. F. Mokbel, C. yin Chow, and W. G. Aref, "The new Casper: Query processing for location services without compromising privacy," in Proceedings of Very Large Databases Conference (VLDB), 2006, pp. 763–774. |