Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

NEW SECURE CONCURRECY MANEGMENT APPROACH FOR DISTRIBUTED AND CONCURRENT ACCESS OF ENCRYPTED CLOUD DATABASES USING DBAAS

Mr.Satish.C.Cholke
Student of M.E Computer,Department of Computer Engineering VACOE, Savitribai Phule Pune University, Ahmednagar,Maharastra(India) Email: cholkesatishchangdeo@gmail.com.

Prof.S.B.Natikar.
Assistant Professor in Department of Computer Engineering, VACOE, Savitribai Phule Pune University, Ahmednagar, Maharastra (India), Email: sbnatikar5@gmail.com.

ABSTRACT
Handover the critical data to the cloud provider should have the guarantee of security and availability for data at rest, in motion, and in use. Many alternatives systems exist for storage services, but the data confidentiality in the database as a service paradigm are still immature. We propose a novel architecture that integrates cloud database services paradigm with data confidentiality and executing concurrent operations on encrypted data. This is the method supporting geographically distributed clients to connect directly and access to an encrypted cloud database, and to execute concurrent and independent operations by using modifying the database structure.
The proposed architecture has also the more advantage of removing intermediate proxies that limit the flexibility, availability, and expandability properties that are inbuilt in cloud-based systems. The efficacy of the proposed architecture is evaluated by theoretical analyses and extensive experimental results with the help of prototype implementation related to the TPC-C standard benchmark for various categories of clients and network latencies. We propose a multi-keyword ranked search method for the encrypted cloud data databases, which simultaneously fulfill the needs of privacy requirements. The proposed scheme could return not only the exact matching files, but also the files including the terms latent semantically associated to the query keyword.

KEYWORDS: Cloud Computing, DBaaS , Cloud Databases, Database As A Service, Ranked Search, Depot, Encrypted Cloud, Homomorphism Encryption, SQL Queries

INTRODUCTION
Cloud based services are becoming popular as they are providingavailability and scalability at low cost. While providing high availability and scalability, placing critical data to cloud poses many security issues. For avoiding these security issues the data are stored in the cloud database in an encrypted format. The encrypted cloud database allows the execution of SQL operations by selecting the encryption schemes that support SQL operators. Encrypted cloud database permits different types of accesses such as distributed, concurrent, and independent. One of the architecture DBaaS Database-as-a-service (DBaaS) is good for two reasons. First, due to economies of scale, the hardware and energy costs incurred by users are likely to be much lower when they are paying for a share of a service rather than running everything themselves. Second, the costs incurred in a well-designed DBaaS will be proportional to actual usage -this applies to both software licensing and administrative costs. The latter are often a significant expense because of the specialized expertise required to extract good performance from commodity DBMSs. By centralizing and automating many database management tasks, a DBaaS can substantially reduce operational costs and perform well.In this paper we define a new scheme named Latent Semantic Analysis (LSA)-based multi-keyword ranked search which supports multi-keyword latent semantic ranked search. By using LSA, the proposed scheme could return not only the exact matching files, but also the files including the terms latent semantically associated to the query keyword.

RELATED WORKS
W. Jansen and T. Grance [1] presented a framework to understand more customizable privacy-issues with composite services. Their approach can be summarized as follows: When a consumer provides data to a service provider, He has to ensure that the information she provides will be used in a consistent manner with his privacy policies. To verify if this will be the case, the client can request a model of the service. The model the examine the manner in which the composite service uses the clients data.

P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin and M. Walfish [2] describe the design, implementation, and evaluation of Depot, a cloud storage system that minimizes trust assumptions. Depot does eliminate trust for updates: a client can always update any object for which it is authorized, and any subset of connected, correct clients can always share updates. Their evaluation suggests that the costs of these guarantees are modest and that Depot can tolerate faults and maintains good availability, latency, overhead, and staleness even when significant faults occur.

H. Hacigu¨mu¨ s¸, B. Iyer and S. Mehrotra [3] have developed and deployed a database service on the Internet, called NetDB2, which is in constant use. In a sense, a data management model supported by NetDB2 provides an effective mechanism for organizations to purchase data management as a service, thereby freeing them to concentrate on their core businesses.

C. Gentry [4] proposed a fully homomorphism encryption scheme i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. First, they provided a general result – that, to construct an encryption scheme that permits evaluation of arbitrary circuits. Next, they describe a public key encryption scheme using ideal lattices that is almost boots trappable.

H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra [5] Executing SQL over Encrypted Data in the Database-Service-Provider Model. It introduces several challenges, an important issue being data privacy. It is in this context that they specifically address the issue of data privacy.

SYSTEM DESIGN

We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data.This is the very good method that supporting geographically distributed users to access an encrypted cloud database directly and to perform concurrent and distributed by modifying the database structure with fine-grain encryption method.

The system model is considering three entities, as in Fig. 1: the data owner, the data user and the cloud server. Data owner has a collection of data documents and a set of distinct keywords is extracted from the Data collection D. At first the data owner will construct an encrypted index I that searchable from the data collection D. Then, the data owner uploads both the encrypted index I and the encrypted data collection C to the cloud server system. Data user provides t keywords for the cloud server. The cloud server only sends back top-l files that are most relevant to the search query.

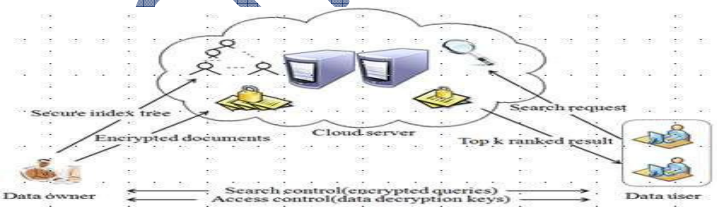

Figure 1- System Architecture

ADVANTAGES OF PROPOSED SYSTEM

The proposed architecture has no need to modify the cloud database, and it is immediately applicable to present cloud DBaaS systems, like experimented PostgreSQL Plus Cloud Database, Windows Azure and Xeround.

There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithm. It sure that the system supports the data confidentiality by allowing a cloud database server to execute concurrent SQL operations not only read or write, but also modifications to the database structure over encrypted data. It allows the same availability, elasticity, and scalability of the original cloud DBaaS because it does not require any intermediate proxies or server systems.

METHODOLOGY

A) Setup Phase

Here describe how to starts the secure DBaaS architecture from a cloud database service acquired by a tenant from a cloud provider. It is consider that the DBA generates the metadata storage table that at the beginning contains just the metadata of the databases, and not the table metadata.

B) Metadata Module

This section describes that, we implements the Meta data. So our system has no needs of any trusted parties or a trusted proxy because tenants data and metadata stored by the cloud database are always encrypted by using fine-

grain encryption technique. In this module, we design such as Tenant data, data structures, and metadata must be encrypted before exiting from the client.

C) Sequential SQL Query Operations

At first the client will connect with the cloud DBaaS for authentication purposes. The Secure DBaaS has belief on standard authentication and authorization methods provided by the original DBMS server. After the authentication, a user interacts with the cloud database through the Secure DBaaS client.

D) Concurrent SQL Operations

The support to concurrent execution of SQL squares issued by many independent and geographically distributed clients is one of the most important benefits of Secure DBaaS with respect to state-of-the-art solutions

3.2.1 Methods for Multi-Keyword Ranked Search

The existing systems like exact or fuzzy keyword search, supports only single keyword searching method. These methods doesn't access the relevant data to users query therefore multi-keyword ranked search over encrypted cloud data having a very challenging approaches. To fulfil these challenges of effective search method, effective and flexible searchable policies are proposed that supports multi-keyword ranked searching technique. In this approach we used the VSM, The Vector Space Model (VSM) is used to produce document index and that is to say that each document is represented as a vector where each dimension value is the Term Frequency (TF) weight of its related keyword. A new vector is also generated in the query phase. The vector has the same dimension with document index and its each dimension value is the Inverse Document Frequency (IDF) weight. Then cosine measure can be used to calculate similarity of one document to the search query.

The equation for finding the F- Measure is:

$$F = \frac{2 \cdot precision \cdot recall}{precision + recall}$$

Multi-keyword Ranked Search: It provides multi-keyword query with support result ranking.Privacy-Preserving: Our scheme is designed to meet the privacy requirement and prevent the cloud server from learning additional information from index and trapdoor.

PERFORMANCE ANALYSIS

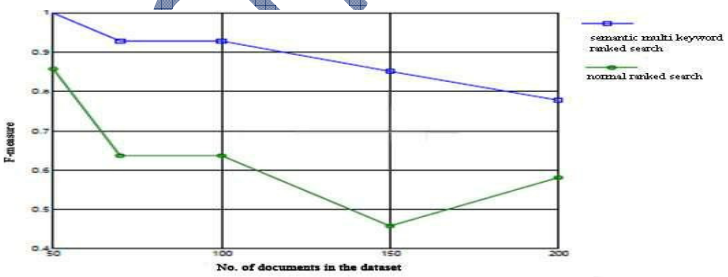

Fig. 2. Comparison of two searches

1) Index Confidentiality Approach. The index must store with the TF values of keywords. Thus, the index stored in the cloud server needs to be encrypted;

2) Trapdoor Unlink ability. The relationship between trapdoors should not be able to deduce by sever.

3) Keyword Privacy System. The server can not disturb the keywords from query, that index by analyzing the statistical information like term frequency.

CONCLUSION

We propose innovative system architecture that achieving confidentiality with integrity of data stored in public cloud databases. Unlike state-of-the-art approaches, our solution does not depends on an intermediate proxy servers systems that can be responsible for a single point of failure and a bottleneck conditions that limiting availability and scalability of today's cloud database services. A large part of the research includes implementable solutions to support concurrent SQL operations including statements modifying the database structure on encrypted cloud data

issued by heterogeneous and possibly geographically dispersed clients. The proposed architecture no need to modify the existing cloud database and it can be directly applicable to any existing cloud DBaaS, such as the experimented PostgreSQL Plus Cloud Database, Windows Azure , and Xeround. There are no any practical limits to extend this system to another platform. We can easily include new encryption techniques. It is widely analysing that experimental results related with the TPC-C standard benchmark show that the performance impact of data encryption on response time becomes negligible because it is masked by network latencies that are typical of cloud scenarios. These performance results open the space to future improvements that we are investigating.

REFERENCES

[1] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication 800-144, NIST, 2011.
[2] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud Storage with Minimal Trust," ACMTrans. Computer Systems, vol. 29, no. 4, article 12, 2011.
a. H. Hacigu¨mu¨s¸, B. Iyer, and S. Mehrotra, "Providing Database as a Service," Proc. 18th IEEE Int'l Conf. Data Eng., Feb. 2002.C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory of ComputingMay 2009.
[3] H. Hacigu¨mu¨s¸, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.
[4] A. Arasu, S. Blanas, K. Eguro, R. Kaushik, D. Kossmann, R. Ramamurthy, and R. Venkatesan, January 2013, "Orthogonal security with cipher base," in Proc. of the 6th Conference on Innovative Data SystemsResearch.
[5] A. Boldyreva, N. Chenette, and A. O'Neill, August 2011, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. of the Advances in Cryptology–CRYPTO 2011,Springer.
[6] "Amazon Elastic Compute Cloud (Amazon Ec2),"AmazonWebServices (AWS),http://aws.amazon.com/ec2.
[7] J. L. DautrichJr and C. V. Ravishankar, March 2013, "Compromising privacy in precise query protocols," in Proc. of the 16th ACM International Conference on Extending Database Technology.
[8] L. Ferretti, M. Colajanni and M. Marchetti, December 2012, "Supporting Security and Consistency for Cloud Database,", in Proc. Fourth Int'l Symp. Cyberspace Safety and Security.
[9] Luca Ferretti, Michele Colajanni, and MircoMarchetti, February 2014, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", VOL. 25, NO. 2.
[10] M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, September 2013, "AS5:A secure searchable secret sharing scheme for privacy preserving database outsourcing," in Proc. of the 5th International Workshop on Autonomous and Spontaneous Security. Springer,.
[11] "PostgresPlus Cloud Database," EnterpriseDB, http://enterprisedb.com/cloud-database.
[12] M. Yabandeh and D. G´omez Ferro, April 2012 , "A critique of snapshot isolation," in Proc. of the 7th ACMeuropean conference on Computer Systems,.
[13] "Xeround: The Cloud Database," Xeround.
[14] Zhangjie Fu, Xingming Sun, Nigel Linge and Lu Zhou, "Achieving Effective Cloud Search Services: Multikeyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query", IEEE Transactionson Consumer Electronics, Vol. 60, No. 1, February 2014

BIOGRAPHY

Mr. CholkeSatish.C received her B.E. in Information Technology Engineering FromSavitribai Phule Pune University, India in 2012.He is pursuing M. E. in Computer Engineering at Vishvabharati Academies College of Engineering, Ahmednagar, affiliated to Savitribai Phule Pune University, Maharashtra, India. His area of research interest is in Cloud Computing.

S.B.Natikaris presently working as Assistant Professor in Dept. of Computer Engineering, Vishvabharati AcademiesCollege of Engineering, Ahmednagar, and Maharashtra, India. His area of research interest is in Cloud Computing.