ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Distributed Independent Competitor Analysis and Access to Databases Encrypted Cloud

Srikanth Bathini
M.Tech,
Dept of Computer Science Engineering,
Prasad College of Engineering.

N.Venkateshwarlu
Assistant Professor,
Prasad College of Engineering.

ABSTRACT:

Establishment of critical data in the hands of a cloud provider should come with the guarantee of security and availability of data at rest, in motion and in use. There are several alternatives for storage services, while the confidentiality of data solutions for the database as a paradigm of services are still immature. We offer a new architecture that integrates cloud services database with data privacy and the ability to perform simultaneous operations on encrypted data. That it is the first solution for customer service for geographically distributed directly connect to an encrypted cloud database and perform simultaneous and independent operations, including those that alter the structure of the database. The proposed architecture has the advantage of eliminating the intermediate proxy that limits the flexibility, availability and scalability are inherent in cloud-based solutions. The proposed architecture performance is evaluated by theoretical analysis, and extensive experimental results based on the performance of the prototype object of standard benchmark TPC-C for different number of customers and network latencies.

INTRODUCTION:

Original raw data should be accessed only by persons of trust that does not include cloud providers, brokers and the Internet; in an unprotected environment, the data must be encrypted. These objectives have different levels of complexity, depending on the type of cloud services. There are several solutions that provide privacy for archiving as a paradigm of services while guaranteeing the confidentiality of data in the database as a service (DBaaS) paradigm is still an open research area. Cannot apply fully homomorphic encryption systems because of their excessive complexity. We proposed a new computer architecture that integrates cloud services database with data privacy and the ability to perform simultaneous operations on encrypted data. This is the first solution for customer service geographically distributed to connect directly to the cloud encrypted database and perform simultaneous and independent operations, including changes to the structure of the database. The proposed architecture has the advantage of eliminating the intermediate proxy that limits the flexibility, availability and scalability are inherent in cloud-based solutions. DBaaS Secure offers several unique features that distinguish it from previous work in the field of security for remote database services.

The proposed architecture requires no changes to the database of clouds and apply immediately DBaaS existing cloud data as experienced cloud PostgreSQL more basic, Windows Azure and Xeround theoretical and practical constraints to expand our solution to other platforms and include new algorithm.It encryption ensures data confidentiality, which allows the server cloud database to perform SQL operation competitors (not only for read / write but also change the structure of the database) provides data.It more encrypted same availability, resilience, and scalability of cloud DBaaS original because it requires no intermediate server.

SYSTEM PRELIMINARIES:

SETUP PHASE:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We describe how to initialize DBaaS secure architecture as a service cloud database acquired by the tenant to the provider cloud. We assume that the DBA creates storage metadata table, which initially contains only metadata database, not metadata table. The DBA is responsible metadata database protected DBaaS customers using cryptographic keys generated randomly for all combinations of data types and kinds of encryption and stores them in the table metadata storage after encryption master key. Then DBA allocates main key to legitimate users. policies to control user access are managed by the DBA through a standard language for data control, since in an encrypted database. The next steps DBA creates tables in an encrypted database.

META DATA MODULE:

In this module, we develop metadata. So our system does not require a trusted agent or proxy trust because the tenants of data and metadata stored in the database of the cloud are always encrypted.In this module, we design data as tenants, data structures and metadata should be encrypted before leave client.The managed by SecureDBaaS information includes encrypted data encrypted data encrypted metadata and metadata. unencrypted data is information that the tenant wants to store and process in DBaaS.SecureDBaaS cloud customers from distance also produce a set of metadata, including information required to encrypt and decrypt data, and other administrative information. Even metadata is encrypted and stored in the cloud DBaaS.

SEQUENTIAL SQL OPERATIONS:

Contact former client DBaaS cloud authentication. DBaaS Secure authentication level dependent and pro-state approval process for the server DBMS original. After approval, a user interacts with the database in the cloud DBaaS Secure client. DBaaS Secure analyzes the original mission to identify and tables are involved and to retrieve metadata from cloud database. The metadata decrypted by the master key and the data is used to translate the original plain SQL query into a database of works on Windows XP.

Translated activities are not common database (table and column names) or data plain bearings. However, they are valid SQL operations, Secure client DBaaS may remove the cloud database. Translated activity is then revealed by the tenant cloud database data over Windows XP. Since there is a correspondence between the tables and regular tables Windows XP one-to-one, it is possible to looga prevent you trust user database access or change the information about tenants, some by providing the right contains the tables of some a. User privileges are automatically controlled by database unreliable cattle cloud. The results of the question translated, including cattle and tenant information received by the client metadata Secure DBaaS, decrypted by the user. the complexity of the translation process depends on the type of SQL statement.

CONCURRENT SQL OPERATIONS:

Support the execution of SQL statements in accordance with the number of independent (and possibly geographically distributed) client is one of the biggest advantages of DBaaS Secure solution compared to the state-of-the-art. Our architecture ensures coherence between tenant data confidentiality and strive for the goal, it is damaged or out-of-date metadata logo to prevent customers from decrypting confidential data tenants resulting in permanent loss of data. A full analysis of the problems and possible solutions related activities in accordance with the SQL data on tenants confidential. Here we noted the importance of the two classes of statements supporting DBaaS Secure: SQL operations do not cause a change in the structure of the database, such as reading, writing and updating; activities involving changes to the database structure through the creation, modification and removal of the database table (data definition of working layer) .

RELATED WORK:

Secure DBaaS offers original features small, who are already working in the field of security services to a variety of remote database. It guarantees the confidentiality of information, Cloud database in

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

accordance with the SQL Server implementation (not only read / write, or update database structure) during the data confidential. It provides access to the same force, and scalability of the cloud DBaaS original does not require any central server. response times are affected by the cost of certain cryptographic operations center at SQL load network. More customers, perhaps geographically, to be simultaneously available and independent database cloud service. It does not require broker or agent is confident reliable, because tenants data and metadata stored in the database is always a cloud encrypted. It compatible with most popular server database connections, and can be used on different DBMS implementations, because the solution to all the database agnostic. File System cryptographic and secure storage solutions represent the first job in this area. We do not detail the number of letters and because they do not support the calculation of confidential data. different ways to ensure confidentiality share some information between different services and take advantage of the secrets to share.

So, they prevent the cloud service to read your piece of data or information provider can back up into the clouds. It is recommended that the first step which makes it possible to make the volume of requests for information and services into a solid. Secure DBaaS Unlike these solutions, it does not require the use of multiple cloud providers, and uses SQL-aware encryption algorithms to support SQL functions most confidential data. Secure DBaaS close working relationship used to protect the confidentiality of the information management database unreliable.

In this case, the main problem is to address the cryptographic techniques that can be applied to the eye because DBaaS standard SQL DBMS can only write data operations. Some DBMS engines allows you to encrypt data via file system feature called Transparent Data confidentiality. This feature is possible to build more trust DBMS untrusted storage. However, DBMS believed and decrypts the data before using them. Therefore, this method does not mean DBaaS, SecureDBaas because we assume that the cloud service is unreliable. Other solutions, such as [18], which allows implementation of many confidential data. These systems to preserve the confidentiality of information in cases where the DBMS is not reliable; However, they need a DBMS engine modified and are not compatible with the DBMS software (both commercial and open source) used by a cloud service provider. Meanwhile, SecureDBaaS compatible with standard motors DBMS, which allows tenants to build secure cloud DBaaS seats database cloud services already available. For this reason, they SecureDBaaS additional means to protect the confidentiality of the information unreliable on encryption techniques SQL DBMS implementation allow more data intelligence, and is compatible with standard DBMS engines. However, the designs of these solutions is based on representative and reliable medium to send between each client and server DBMS unreliable.

Access to the proposed model, the authors employed a data DBaaS data blocks where each item of data. When you need information that belongs to the block must represent a reliable block of all to read and analyze the information that we needed to block one. Therefore, this design choice is to replace the original SQL serious operation on every client, which causes the value of fixed and DBMS server and proxy trust. Other papers presented to the public and to increase the subset of SQL support workers, but they share the same architecture represented on the problems within. On the other hand, they do SecureDBaaS Windows XP operations data via SQL encryption algorithms intentionally.

CONCLUSION:

We propose a new architecture that guarantees the confidentiality of the information stored in the public cloud database. In contrast to state-of-the-art system, our solution does not rely on an agent to look at the middle point of a neck of the bottle and a failure to reduce the availability and scalability of cloud database standard. Much of the research include solutions to support the activities of SQL at the same time (including the statement that changes the structure

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

of the database) so that data encrypted on by consumers heterogeneous and possibly geographically dispersed. architecture proposed requires no changes to the database in the cloud, and it is urgent that can be applied to DBaaS cloud are tested PostgreSQL Plus Cloud Base No limit to the theoretical and to extend our solutions to other platforms and a new encryption algorithms. It is worth to note that the results of the test based on TPC-C benchmark standard shows that the effects of the confidentiality of data in the form of response time would be negligible, because the network load from a roadside bomb in cases clouds are common. In particular, once read and write operations, not out on the base of the structure because of the negligible encoded. Dynamic support cases characterized by a (possibly) simultaneously changes the structure of the database, but at the expense of high-cost accounting. These results pave the way for future improvements in screening.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing," Comm. of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication 800-144, NIST, 2011.

[3] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, "SPORC: Group Collaboration Using Untrusted Cloud Resources," Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[4] J. Li, M. Krohn, D. Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation, Oct. 2004.

[5] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud Storage with Minimal Trust," ACM Trans. Computer Systems, vol. 29, no. 4, article 12, 2011.

[6] H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra, "Providing Database as a Service," Proc. 18th IEEE Int'l Conf. Data Eng., Feb. 2002.

[7] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory of Computing, May 2009.

[8] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles, Oct. 2011.

[9] 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.

[10] J. Li and E. Omiecinski, "Efficiency and Security Trade-Off in Supporting Range Queries on Encrypted Databases," Proc. 19th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, Aug. 2005.

[11] E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, July/Aug. 2006.

[12] D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, "Database Management as a Service: Challenges and Opportunities," Proc. 25th IEEE Int'l Conf. Data Eng., Mar.-Apr. 2009.

[13] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.

[14] A. Shamir, "How to Share a Secret," Comm. of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[15] M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, "AS5: A Secure Searchable Secret Sharing

Scheme for Privacy Preserving Database Outsourcing," Proc. Fifth Int'l Workshop Autonomous and Spontaneous Security, Sept. 2013.

[16]"Oracle Advanced Security," Oracle Corporation, http://www.oracle.com/technetwork/database/options/advanced-security, Apr. 2013.

[17]G. Cattaneo, L. Catuogno, A.D. Sorbo, and P. Persiano, "The Design and Implementation of a Transparent Cryptographic File System For Unix," Proc. FREENIX Track: 2001 USENIX Ann. Technical Conf., Apr. 2001.

[18]E. Damiani, S.D.C. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Balancing Confidentiality and Efficiency in Untrusted Relational Dbmss," Proc. Tenth ACM Conf. Computer and Comm. Security, Oct. 2003.

[19]L. Ferretti, M. Colajanni, and M. Marchetti, "Supporting Security and Consistency for Cloud Database," Proc. Fourth Int'l Symp. Cyberspace Safety and Security, Dec. 2012.

[20]"Transaction Processing Performance Council," TPC-C, http:// www.tpc.org, Apr. 2013.