IJRRECS/November 2015/Volume-3/Issue-11/4881-4885 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A SECURITY ANALYSIS OF INDEPENDENT DATA ACCESS CONTROL IN DISTRIBUTED CLOUD SERVICES

Kota Anusha[1], Ch.Kiran[2]

[1]M.Tech Student, Dept of CSE, Turbomachinery Institute of Technology & Sciences, Hyderabad, T.S, India
[2]Assistant Professor, Dept of CSE, Turbomachinery Institute of Technology & Sciences, Hyderabad, T.S, India

ABSTRACT:

The projected structural design has advantage of eliminating intermediate proxies that limit elasticity, accessibility, as well as scalability properties that are inherent in cloud-based solutions. Secure database as a service construct traditional cryptographic methods, isolation methods, and new strategies for managing of encrypted metadata on untrustworthy cloud database. A innovative construction that combines cloud database services by data confidentiality and option of executing simultaneous operations on encrypted data. By removal of any trustworthy intermediate server permit secure database as a service to achieve the identical accessibility, trustworthiness, and flexibility levels of a cloud database as a service. It assures data privacy by allowing a cloud database server to perform concurrent operations over encrypted data. The system provides a number of original features that differentiate it from earlier work in the field of security for isolated database services.

Keywords: Encrypted, Cryptographic, Cloud system, Secure database as a service, Intermediate server.

1. INTRODUCTION:

We put forward Secure database as a service as effective solution that permit cloud tenants to take full benefit of database as a service qualities, for instance availability, trustworthiness, and elastic scalability, devoid of exposing unencrypted information towards cloud provider [1]. There are quite a lot of solutions that ensures confidentiality for storage as a service concept while assuring privacy in database as a service paradigm is still an area of research. A huge set of experiments on basis of real cloud platforms reveal that secure database as a service is instantly valid to any DBMS since it requires

no alteration to the cloud database services. The option of combining accessibility, flexibility, and scalability of a distinctive cloud database as a service by means of data confidentiality is verified all the way through a prototype of secure database as a service that supports implementation of simultaneous and self-regulating operations to secluded encrypted database from numerous geographically distributed clients as in any unencrypted database as a service setup. It is compatible with most accepted relational database servers, and it is appropriate to several database implementations since all adopted solutions are database agnostic [2][3]. Secure database as a service put together existing cryptographic methods, isolation methods, and new strategies for managing of encrypted metadata on untrustworthy cloud database. Secure database as a service differs from other works since it does not necessitate the use of numerous cloud providers, and makes usage of SQL-aware encryption algorithms to maintain the implementation of most general SQL operations on encrypted information. Secure database as a service share strongly to works by means of encryption to defend data managed by untrustworthy databases. In such a case, a most important issue to deal with is that cryptographic techniques cannot be functional to criterion database as a service since DBMS can merely implement SQL operations above plaintext data.

2. METHODOLOGY OF SECURE DATABASE AS A SERVICE:

This is initial solution that support geographically dispersed clients to join directly towards an encrypted cloud database, and to carry out simultaneous and independent operations including those changing database structure. The proposed structural design has benefit of eliminating intermediate proxies that limit elasticity, accessibility, as well as scalability properties that are inherent in cloud-based solutions. The Secure database as a service structural design is modified to cloud platforms and does not initiate any intermediary proxy among the client and cloud provider. We recommend a new architecture that combine cloud database services by data confidentiality and option of executing simultaneous operations on encrypted data. Eliminating any trustworthy intermediate server permit secure database as a service to achieve the identical accessibility, trustworthiness, and flexibility levels of a cloud database as a service. Unlike Secure database as a service, architectures depending on a trustworthy intermediate proxy do not maintain the most typical cloud situation where

geographically dispersed customers can simultaneously provide read/write operations as well as data structure modifications towards a cloud database. Secure database as a service provides quite a lot of original features that distinguish it from earlier work in the field of security for isolated database services. It assures data privacy by allowing a cloud database server to perform concurrent operations over encrypted data. It does not necessitate a trusted broker since tenant data as well as metadata stored by cloud database are constantly encrypted. It is well-suited with most accepted relational database servers, and it is appropriate to several database implementations since all adopted solutions are database agnostic [4]. It provides the similar availability, flexibility, and scalability of original cloud database as a service since it does not necessitate any intermediate server and it is attuned with criterion DBMS engines, and permit tenants to construct sheltered cloud databases by leveraging cloud database as a service services that are already obtainable.

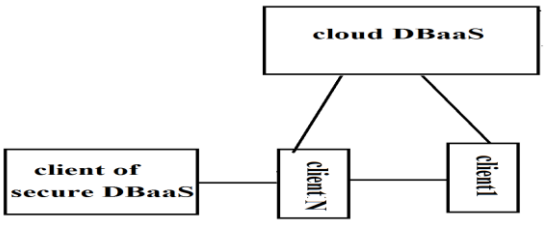

Fig1: overview of secure database as a service.

3. MODELLING OF PROPOSED SYSTEM:

We assume that a tenant organization obtain a cloud database service from an untrustworthy database as a service provider. The tenant then deploys one or additional machines and set up a Secure database as a service client on each of them. This client permit a user to connect to the cloud database as a service to manage it, to read as well as write data, and even to generate and change the database tables subsequent to creation. The information that is managed by the introduced system includes plaintext data, metadata, encrypted metadata and encrypted data. Plaintext data comprises of information that a tenant wants to accumulate and practice a little in the cloud d Secure database as a service is considered to permit numerous and self-determining clients to attach directly to unreliable cloud database as a service devoid of any intermediate server. Database as a service. To prevent an unreliable cloud provider from contravening confidentiality of tenant data stored in plain form, the secure database system adopts abundant cryptographic techniques to alter plaintext data into encrypted tenant information in addition to encrypted tenant data structures since even names of the tables as well as their columns have to be encrypted [5]. This is first explanation that support geographically dispersed clients to join directly

towards an encrypted cloud database, and to carry out simultaneous and independent operations including those changing database structure. Secure database as a service system clients construct a set of metadata consisting of information necessary to encrypt as well as decrypt data. Secure database as a service moves away from traditional architectures that accumulate just tenant data within the cloud database, and accumulate metadata in client machine or divide metadata among cloud database as well as a trusted proxy. The Secure database as a service structural design is modified to cloud platforms and does not initiate any intermediary proxy among the client and cloud provider. During consideration of situations where numerous clients can access similar database simultaneously, these previous solutions are quite ineffective [6]. Solutions on basis of a trustworthy proxy are more reasonable, but they commence a system blockage that reduces accessibility, flexibility, and scalability of cloud database services. Secure database as a service recommend a different approach where the entire data as well as metadata are stored in cloud database. It does not require any intermediate server and it is attuned with criterion database engines, and permit tenants to construct sheltered cloud databases by leveraging cloud database as a service services that are already obtainable. Its clients can recover the essential metadata from untrustworthy database with the intention that numerous instances of Secure database as a service client can access to untrustworthy cloud database separately with the assurance of same accessibility and scalability properties of representative cloud database as a service.

4. CONCLUSION:

The system constructs existing cryptographic methods, isolation methods, and new strategies for managing of encrypted metadata on untrustworthy cloud database. The proposed design has advantage of eliminating intermediate proxies that limit elasticity, accessibility, as well as scalability properties that are inherent in cloud-based solutions. Secure database as a service as effective solution that permit cloud tenants to take full benefit of database as a service qualities, for instance availability, trustworthiness, and elastic scalability, devoid of exposing unencrypted information towards cloud provider. Secure database as a service makes available numerous original features that distinguish it from earlier work in the field of security for isolated database services. This is first solution that sustains geographically dispersed clients to join directly towards an encrypted cloud database, and to carry out

simultaneous and independent operations including that changing database structure. It is well-matched with most established relational database servers, and it is suitable to several database performances.

REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.