IJRRECS/June 2015/Volume-3/Issue-6/4171-4175 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IMPLEMENTATION OF APPROACH FOR MAINTAINING DATA CONFIDENTIALITY IN DATABASE SERVICES

H.M.Sasya Sree[1], A.Radha Rani[2]

[1]M.Tech Student, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

ABSTRACT:

The outlook of combining reliability, accessibility and flexible scalability of a representative cloud database as a service with data confidentiality is verified all the way through secure database as a service. Secure database as a service relates strictly to works by means of encryption to defend data that is managed by untrusted databases. Secure database as a service is instantaneously appropriate to any DBMS as it requires no alteration to cloud database service. We put forward secure database as a service as solution that permits cloud tenants to take complete benefit of database as a service qualities and assures privacy of data stored within databases of public cloud. Unlike modern approaches, our solution does not depend on intermediate proxy that we believe a single point of breakdown and a blockage limiting accessibility as well as scalability of representative cloud database services. Secure DBaaS put together existing cryptographic methods, isolation and novel strategies in support of managing encrypted metadata on untrusted cloud database. Secure DBaaS makes available quite a lot of original features that distinguish it from earlier work in field of security for distant database services. It is well-suited with the majority of relational database servers, and it is valid towards several DBMS operations since all approved solutions are database agnostic. It assures data confidentiality by means of permitting a cloud database server to carry out concurrent SQL procedures over encrypted data.

Keywords: Secure database as a service, DBMS, Public cloud, Metadata, SQL, Data confidentiality.

1. INTRODUCTION:

In the context of cloud, making sure of data confidentiality is of principal importance where important data is positioned within untrusted third parties [1]. There are a lot of work out were carried out for ensuring confidentiality for storage as a service concept although guaranteeing privacy within database as a service idea is still an open areaof research. Several approaches assurances some confidentiality by means of distributing data between several providers moreover by taking benefit of secret sharing. Secure database as a service relates strictly to works by means of encryption to defend data that is managed by untrusted databases. We put forward Secure database as a service as solution that permits cloud tenants to take complete benefit of database as a service qualities, for instance reliability, accessibility and flexible scalability, devoid of exposing unencrypted information to cloud provider [2][3]. The architecture that was designed was motivated by means of objective of threefold such as: to permit numerous, independent, as well as geographically distributed clients to carry out synchronized operations on encrypted data, comprising SQL statements that alter database structure; to maintain data privacy as well as constancy at client as well as cloud level; to get rid of any intermediate server among cloud client as well as cloud provider. Secure database as a service is tailored towards cloud platforms and does not set up any intermediary proxy among cloud provider and client. Elimination of any trustworthy intermediate server permits Secure DBaaS to attain reliability, accessibility and flexible scalability levels of a cloud database as a service. Secure DBaaS recommend a different method where the entire data as well as metadata are accumulated within cloud database. Unlike Secure database as a service, architectures which depend on trustworthy intermediate proxy do not maintain most distinctive cloud circumstances where geographically distributed clients issue read or write operations to cloud database. Secure database as a service is instantaneously appropriate to any DBMS as it requires no alteration to cloud database service.

2. METHODOLOGY:

The prospect of combining reliability, accessibility and flexible scalability of a representative cloud database as a service with data confidentiality is verified all the way through secure database as a service

that maintains implementation of concurrent as well as independent operations to distant encrypted database from numerous geographically dispersed clients as in any unencrypted database as a service setup. Secure DBaaS put together existing cryptographic methods, isolation and novel strategies in support of managing encrypted metadata on untrusted cloud database. Secure DBaaS makes available quite a lot of original features that distinguish it from earlier work in field of security for distant database services. It provides the same reliability, accessibility and flexible scalability levels of a cloud database as a service because it does not necessitate any intermediate server [4]. It is well-suited with the majority of relational database servers, and it is valid towards several DBMS operations since all approved solutions are database agnostic. It assures data confidentiality by means of permitting a cloud database server to carry out concurrent SQL procedures over encrypted data. It is well-matched with the majority of DBMS and permits tenants to construct secure cloud databases by means of leveraging cloud database as service that is already obtainable. It does not necessitate a trusted broker since tenant data as well as metadata stored by the cloud database are constantly encrypted. Secure DBaaS permits the carrying out of operations above encrypted data all the way through SQL-aware encryption algorithms. Secure DBaaS maintains distributed clients who issues concurrent SQL operations to the similar database and probably to same data.

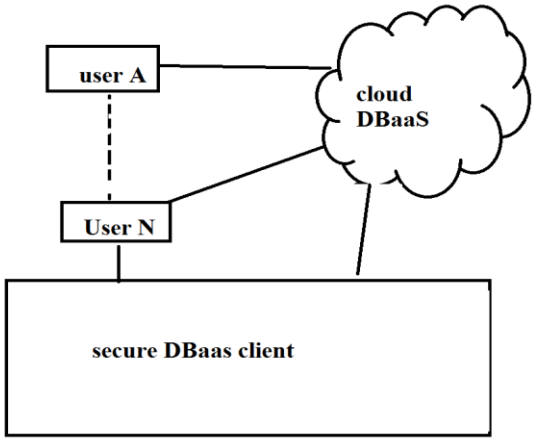

Fig1: An overview of Secure DBaaS

3. AN APPROACH TOWARDS SECURE DATA BASE AS A SERVICE:

We put forward secure database as a service as solution that permits cloud tenants to take complete benefit of database as a service qualities and assures privacy of data stored within databases of public cloud. Unlike modern approaches, our solution does not depend on intermediate proxy that we believe a single point of breakdown and a blockage limiting accessibility as well as

scalability of representative cloud database services. Secure DBaaS as shown in fig1 recommend a different method where the entire data as well as metadata are accumulated within cloud database [5]. Clients of secure DBaaS can recover essential metadata from the untrusted database all the way through SQL statements, with the intention that numerous instances of secure database as a service client can access to untrusted cloud database autonomously with the assurance of similar reliability, accessibility and flexible scalability properties of distinctive cloud DBaaS. Unlike Secure database as a service, architectures which depend on trustworthy intermediate proxy do not maintain most distinctive cloud circumstances where geographically distributed clients issue read or write operations to cloud database. SecureDBaaS is intended to permit numerous as well as independent clients to fix directly to untrusted cloud DBaaS devoid of any intermediate server. A tenant organization was assumed to get hold of a cloud database from provider of untrusted DBaaS. Tenant subsequently organize one or additional machines and install a secure database as a service client on each of them which permit a user to fix to cloud DBaaS to manage it, to read as well as write data, and even to generate and change the database tables subsequent to creation. The information which is managed by secure database as a service comprises plaintext data, metadata, as well as encrypted metadata. Plaintext data comprises of information that a tenant needs to store as well as process distantly within the cloud database as a service. To put off an untrusted cloud provider from breaking privacy of tenant data stored within plain form, secure database as a service takes on numerous cryptographic methods to make over plaintext data into encrypted tenant information as well as encrypted tenant data structures because still names of tables and columns have to be encrypted [6].

4. CONCLUSION:

We put forward Secure database as a service as solution that permits cloud tenants to take complete benefit of database as a service qualities, for instance reliability, accessibility and flexible scalability, devoid of exposing unencrypted information to cloud provider. Unlike modern approaches, our solution does not depend on intermediate proxy that we believe a single point of breakdown and a blockage limiting

accessibility as well as scalability of representative cloud database services. Unlike Secure database as a service, architectures which depend on trustworthy intermediate proxy do not maintain most distinctive cloud circumstances where geographically distributed clients issue read or write operations to cloud database. Secure DBaaS makes available quite a lot of original features that distinguish it from earlier work in field of security for distant database services. It provides the same reliability, accessibility and flexible scalability levels of a cloud database as a service because it does not necessitate any intermediate server. It is well-matched with the majority of DBMS and permits tenants to construct secure cloud databases by means of leveraging cloud database as service that is already obtainable. It does not necessitate a trusted broker since tenant data as well as metadata stored by the cloud database are constantly encrypted. SecureDBaaS is intended to permit numerous as well as independent clients to fix directly to untrusted cloud DBaaS devoid of any intermediate server.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

[6] H. Berenson, P. Bernstein, J. Gray, J. Melton, E. O'Neil, and P. O'Neil, "A Critique of Ansi Sql Isolation Levels," Proc. ACM SIGMOD, June 1995.