IJRRECS/March 2016/Volume-4/Issue-3/5287-5291 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A NOVEL STRUCTURE FOR ASSURING DATA PRIVACY IN CLOUD DATABASE

Mohammad Eliyas [1], Dr.P.Venkateswarlu[2], S.Sree Hari Raju[3]

[1]M.Tech Student, Dept of CSE, Nagole Institute of Technology & Science, Hyderabad, T.S, India
[2]Professor & HOD, Dept of CSE, Nagole Institute of Technology & Science, Hyderabad, T.S, India
[3]Assistant Professor, Dept of CSE, Nagole Institute of Technology & Science, Hyderabad, T.S, India

ABSTRACT:

There are various methods that make sure of protection for storage service while promising of privacy in database as a service is considered as an important research area till now. Organizing of important data by the cloud provider should give assurance of protecting and accessing of the data in any situation. We employ an approach that assures confidentiality of data that is stored within databases of public cloud. The design makes it associated to works that makes uses encryption to defend data that is managed by databases that are not trustable.

This approach incorporates services of cloud database by means of data privacy and implements synchronized operations on encrypted information. It is compatible with satisfactory database servers and is related to various database functioning since the entire adopted solutions are database agnostic. It put together conventional methods of cryptography schemes, as well as new methods for managing of encrypted metadata on the cloud database that is not trustable.

Keywords: Cloud database, Cryptography schemes, Encrypted, Storage service.

1. INTRODUCTION:

This characteristic helps to construct a trustworthy database service on the storage of which cannot be trusted. Various other services permit implementation of operations on the encrypted information and these helps in preserving of data privacy in situations where database service is not trusted. Several database services present the encryption of data at level of file system by

means of transparent aspect of data encryption [1]. On the other hand these services require modified database service engine and are not well-suited to the database software that is used by the providers of cloud. Various other solutions are present for storage services, whereas the solutions of data privacy for database service are not fully created. We implement an innovative approach that assures confidentiality of data that is stored within databases of public cloud. The proposed approach permits the cloud users to perform various features such as user-friendliness, dependability, as well as scalability, devoid of exposing of unencrypted information for the cloud provider. It can remove intermediate proxies that limit user-friendliness, dependability, as well as scalability, properties that are essential in the solutions of cloud-based. It does not need a confidential broker since tenant data as well as metadata that are stored by cloud database are constantly encrypted; and the proposed system is well-suited with acceptable database servers. The approach is related to various database functioning since the entire adopted solutions are database agnostic [2]. The proposed approach offers several other characteristics and these makes it different from other solutions in security area for remote services of database. It promises data privacy by means of permitting a cloud database server to carry out synchronized operations on encrypted information. Proposed secured database service is personalized towards cloud platforms and will not commence any intermediary proxy among client and cloud provider.

2. METHODOLOGY:

This solution supports distributed clients to bond directly towards an encrypted cloud database, and to perform independent operations. The design was encouraged by means of a threefold objective such as to permit several, autonomous, as well as distributed clients to implement synchronized operations on encrypted information; to protect data privacy and constancy at cloud level; to get rid of any intermediate server among cloud client as well as cloud provider. The design makes it relates to works that makes uses encryption to defend data that is managed by databases that are not believed. The ability of combining of a variety of features such as user-friendliness, dependability, as well as scalability with data privacy is confirmed all

the way through secure database service that helps in implementation of independent operations to isolated encrypted database from numerous distributed clients. The approach differs from existing structures that store tenant information within cloud database, as well as save metadata within client machine. The proposed secured database service put together traditional methods of cryptography schemes, as well as new methods for managing of encrypted metadata on the cloud database that is not trustable [3]. The proposed approach integrates services of cloud database by means of data privacy and implements synchronized operations on encrypted information. Secure database system is well-suited to database engines, and permits tenants to construct effective cloud database by means of managing of cloud services that are previously available. It permits the cloud users to perform various features such as availability, evenness, as well as scalability, devoid of exposing of unencrypted information for the cloud provider [4]. Proposed database service is modified towards cloud platforms and will not commence any intermediary proxy among client and cloud provider.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Various methods assure some privacy by means of distribution of data between several providers and consider secret sharing. The proposed design makes it relates to works that makes uses encryption to defend data that is managed by databases that are not trustable. Ensuring of data privacy in untrustworthy servers is very important and it requires data management options such as original plain data should be available by trustworthy parties that do not comprise cloud providers as well as Internet [5]. We put into practice an innovative approach that assures confidentiality of data that is stored within databases of public cloud. The proposed structural design has benefit of removal of intermediate proxies that limit user-friendliness, dependability, as well as scalability, properties that are essential in the solutions of cloud-based. This supports distributed clients to bond directly towards an encrypted cloud database, and to perform autonomous actions. The approach presents several other characteristics and these makes it different from other solutions in security area for distant services of database. Secure database system is compatible to database engines,

and permits tenants to construct effective cloud database by means of managing of cloud services that are previously available. The design has to permit several, autonomous, as well as distributed clients to implement synchronized operations on encrypted information and should protect data privacy and constancy at cloud level. In the system model as shown in fig1 we assume that tenant organization obtains the service of cloud database from not trustable database service provider. The tenant arranges machines and set up effective database client on each. Client permits user to bond cloud database service to manage it, read and write information, and adjust database tables subsequent to creation. The proposed approach differs from existing structures that store tenant information within cloud database, as well as save metadata within client machine or divide metadata among cloud database as well as trustworthy proxy. During consideration of scenarios in which numerous clients access similar database simultaneously, these earlier solutions are relatively uneconomical. The clients will recover essential metadata from non trustable database all the way through SQL statements, so that numerous clients of database can access to untrustworthy database with assurance of similar user-friendliness, dependability, as well as scalability of representative cloud database. It assures data privacy by means of permitting a cloud database server to carry out synchronized operations on encrypted information and does not need a confidential broker since tenant data as well as metadata that are stored by cloud database are constantly encrypted [6]. It constructs traditional methods of cryptography schemes, as well as new methods for managing of encrypted metadata on the cloud database that is not trustable. The proposed system put forward a different approach in which the metadata are stored within cloud database.

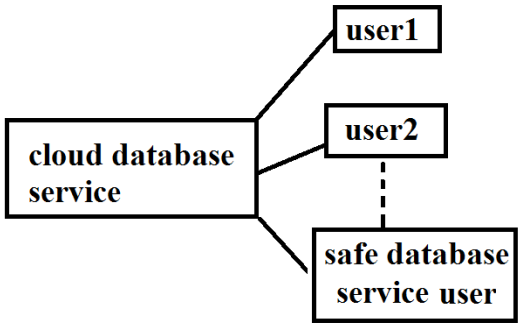

Fig1: Secure Database Service.

4. CONCLUSION:

A variety of methods promises some privacy by means of distribution of data between several providers and considers secret sharing. We execute an innovative approach that assures confidentiality of data that is stored within databases of public cloud. In a cloud circumstance, in which key data is placed in the services of third parties that are not trustable, making sure of data privacy is of vital significance. It offers quite a lot of characteristics and these makes it different from other solutions in security area for remote services of database and supports distributed clients to bond directly towards an encrypted cloud database, and to perform independent operations. The secured databases construct conventional methods of cryptography schemes, as well as new methods for managing of encrypted metadata on the cloud database that is not trustable. It is personalized towards cloud platforms and will not commence any intermediary proxy among client and cloud provider. Proposed system is compatible with satisfactory database servers and is related to various databases functioning since the entire adopted solutions are database agnostic and integrates services of cloud database by means of data privacy and implements synchronized operations on encrypted information.

REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

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

[6] 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.