IJRRECS/January 2016/Volume-4/Issue-1/5170-5174 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IMPLEMENTATION OF DISTRIBUTED ACCESS FOR ENCRYPTED DATA ON CLOUD SYSTEM

N.Vijaya Sunder Sagar[1], Rapelly Nandini[2]

[1]Assistant Professor & HOD, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

[2]M.Tech Student, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

ABSTRACT:

Various approaches were implemented in earlier times for the storage services, whereas the approaches of data confidentiality for database as a service are not properly handled. We put into practice a service of cloud database that promises privacy and implements concurrent operations on encrypted data. Introduction of important data to cloud provider has to assure security as well as accessibility for data. The system constructs traditional schemes of cryptography as well as novel methods for managing of encrypted metadata on untrustworthy cloud database.. Secure database concept functions as initial service that makes tenants of cloud system to benefit of reliability as well as flexible scalability features devoid of exposing unencrypted data towards cloud provider and moreover offers various features that distinguish it from earlier works for remote database services. The proposed secure database service is straight valid towards any of the database service as it requires no change to services of cloud database

Keywords: Secure database service, Security, Cloud database, Cloud provider, Cryptography, Unencrypted, Privacy.

1. INTRODUCTION:

Gathering the reliability, flexibility of cloud database service is confirmed by the secure database concept. It assists in implementation of concurrent as well as independent actions towards isolated encrypted database from lots of distributed clients. We implement a service of cloud database that assures privacy and implements concurrent operations on encrypted data [1]. The proposed approach of secure database concept functions as the initial service that makes tenants of cloud system to benefit of reliability as well as flexible scalability features devoid of exposing unencrypted data towards cloud provider. There are different methods that make sure of confidentiality for storage as a service but assuring of confidentiality in database as a service was not properly managed by any of the earlier methods. The proposed approach of cloud database service is tailored towards cloud platforms and will not initiate any proxy among client as well as cloud provider. This proposed system mainly put together traditional schemes of cryptography as well as novel methods for managing of encrypted metadata on untrustworthy cloud database. Proposed approach makes itself different from other solutions as it does not need usage of numerous cloud providers, and makes usage of encryption algorithms to supporting of operations on encrypted data. The approach of secure database service is straight away valid towards any of the database service as it requires no change to services of cloud database [2][3]. It is identifiable with criterion database engines, and permits tenants to put up protected cloud databases by means of controlling cloud database services. Removal of any trustworthy intermediate server permits the secure database service to gain same level of reliability as well as flexible levels of cloud database.

2. METHODOLOGY:

This element makes it likely to put up a trusted database over untrustworthy storage. The database system is dependable and decrypts data previous than usage and hence, this technique is not suitable towards database situation that is supervised by effective database service that is considered by secure database service, since we suppose that cloud provider is untrustworthy. Secure database functions as the initial service that makes tenants of cloud system to benefit of reliability as well

as flexible scalability features devoid of exposing unencrypted data towards cloud provider. It supports distributed clients to connect to encrypted cloud database and implements concurrent operations on encrypted data. Exclusion of responsible intermediate server permits the secure database service to gain same level of reliability as well as flexible levels of cloud database. The proposed approach does not necessitate a trustworthy broker since tenant data as well as metadata that are stored by cloud database are constantly encrypted. Several database service engines provide the option of encryption of data at level of file system all the way through Transparent Data Encryption feature. It is well-matched with standard database engines, and permits tenants to put up protected cloud databases by means of controlling cloud database services. The approach is compatible with the majority of database servers, and appropriate to various database functioning since all adopted solutions are database agnostic. Proposed secure database service offers various features that distinguish it from earlier works for remote database services [4]. It helps in assuring of data confidentiality by means of permitting of cloud database server to implement synchronized SQL functions on encrypted information. Cryptographic file systems as well as protected storage solutions correspond to the earliest works in this area. It relates closely to works that uses encryption to defend data that is managed by untrustworthy databases. In such situation, important issue to deal with is that cryptographic methods cannot be naı¨vely functional to standard database service since databases services carry out SQL functions on plaintext data [5]. This proposed system construct established schemes of cryptography as well as novel methods for managing of encrypted metadata on untrustworthy cloud database. Proposed cloud database makes itself different from other solutions as it does not need usage of numerous cloud providers, and makes usage of encryption algorithms to supporting of operations on encrypted data.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Approach of secure database has to permit numerous clients to fix directly to untrustworthy cloud database devoid of any intermediate server. The approach does not necessitate a trustworthy broker since tenant data as well as metadata that are stored by

cloud database are constantly encrypted. A service of cloud database that assures privacy was introduced and employs concurrent operations on encrypted data. Proposed approach of secure database is compatible with standard database engines, and permits tenants to put up protected cloud databases by means of controlling cloud database services. The database service that is proposed offers various features that distinguish it from earlier works for remote database services and is straight away valid towards any of the database service as it requires no change to services of cloud database. Approach of cloud database service is tailored towards cloud platforms and will not initiate any proxy among client as well as cloud provider. Approach of secure database put forward a distinct method where the entire data as well as metadata that are stored in cloud database. The clients of proposed database service can get back essential metadata from the untrustworthy database with the intention that numerous instances of secure database client can access to untrustworthy cloud database separately with assurance of similar scalability properties of cloud database. Taking away of any trustworthy intermediate server permits the secure database service to gain same level of reliability as well as flexible levels of cloud database. Secure database service moves away from existing methods that store up tenant data in the system of cloud database, and accumulate metadata in client machine. During consideration of the situations in which several clients access similar database simultaneously earlier solutions are quite ineffective. We consider the security representation that is adopted by literature in this area where tenant users are trustworthy, network is untrustworthy, and cloud provider is honest-but-curious [6]. For prevention of an unreliable cloud provider from violation of privacy of tenant data stored within plain form, the proposed system adopts numerous cryptographic methods to change plaintext data to encrypted tenant data as well as encrypted data structures since even names of tables and their columns have to be encrypted. A tenant organization was assumed to obtain a cloud database service from an untrustworthy database provider. The tenant later installs an effective database service client on each of them and allows for bonding to cloud database service to administer it, to read as well as write data,

and even to change database tables subsequent to creation.

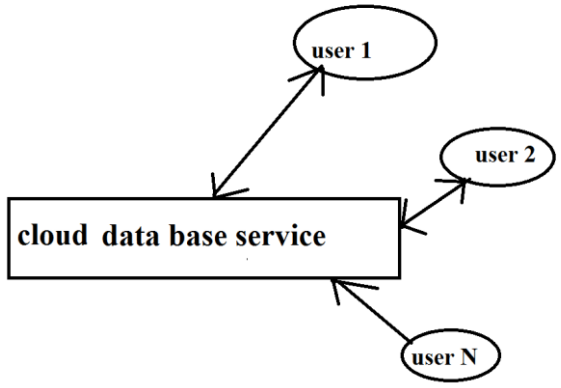

Fig1: proposed database as a service.

4. CONCLUSION:

The secure database service is promptly appropriate towards any of the database service as it requires no change to services of cloud database. Proposed service offers different features that distinguish it from earlier works for remote database services. This system put together usual schemes of cryptography as well as novel methods for managing of encrypted metadata on untrustworthy cloud database. In our work we execute a service of cloud database that assures privacy and implements concurrent operations on encrypted data. Cloud database that was introduced makes itself different from other solutions as it does not need usage of numerous cloud providers, and makes usage of encryption algorithms to supporting of operations on encrypted data. Proposed approach is tailored towards cloud platforms and will not initiate any proxy among client as well as cloud provider. The proposed secure database notion functions as initial service that makes tenants of cloud system to benefit of reliability as well as flexible scalability features devoid of exposing unencrypted data towards cloud provider. It assures data privacy by means of permitting of cloud database server to implement synchronized functions on encrypted information.

REFERENCES

[1] 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.

[2] 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.

[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] 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.

[5] 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.

[6] A. Fekete, D. Liarokapis, E. O'Neil, P. O'Neil, and D. Shasha, "Making Snapshot Isolation Serializable," ACM Trans. Database Systems, vol. 30, no. 2, pp. 492-528, 2005.