Employing of Innovative Approach for Managing of Data on Cloud Server

NAVEEN YERRAMSHETTI
Dept of CS,
Bradley University,
Peoria, Illinois, USA

Abstract: **Various methods are present for storage services, whereas solutions of data privacy for database service are not very effective. Many techniques were introduced in literatures that assure privacy to a certain limit by means of data distribution and by consideration of secret sharing. We make a study on protective database service that acts as major solution allowing cloud tenant to gain various features such as ease of understanding, dependability, and flexibility devoid of revealing of unencrypted data towards cloud provider. Various studies on basis of cloud platforms exhibit that protective database service is valid to any of the database systems as it does not modify services of cloud database. Our solution acts as leading solution that manages distributed clients for connecting towards an encrypted database, and for implementation of self-determining operations.**

Keywords: **Data privacy, Database service, Data distribution, Cloud provider, Storage services, Cloud database.**

I. INTRODUCTION

In a cloud, data is located in Infrastructures of third party that are unreliable and guaranteeing of data confidentiality within this system is very important. Fulfilling of the objectives for assuring of data confidentiality in the cloud system contains several difficulty levels based on cloud services. Several database system engines put forward encryption of data at file system level by a feature of transparent data encryption [1]. A protective database service was introduced for assuring of data privacy that is build up in open cloud databases. Proposed protective database service associates more close to the works that makes use of encryption for protection of data that is manageable by undependable databases. This strategy does not depend on intermediary proxy that considers breakdown and blockage that confines accessibility of representative cloud services. The database service that was proposed has a benefit of eliminating intermediate proxies that confine to ease of understanding, dependability, and flexibility properties that are basically important in cloud solutions. Proposed database service does not necessitate alterations to cloud database, and it is instantly appropriate towards existing cloud databases.

II. METHODOLOGY

We put into practice a shielding database service that acts as foremost solution allowing cloud tenant to gain various features such as ease of understanding, dependability, and flexibility devoid of revealing of unencrypted data towards cloud provider. Our solution as foremost solution that manages distributed clients for connecting towards an encrypted database, and for implementation of self-determining operations [2][3]. Protective database service is well-matched with standard database engines, and permits cloud tenant to gain various features to make a protective database service by means of controlling of cloud data services that are already existed. Protective database construct cloud services by means of data privacy as well as choice of synchronized operations on encrypted information. The database service that was proposed secures data privacy by permitting of cloud server to perform concurrent operations above encrypted information. Protective database service is well-matched with relational database servers, and it is well-matched to several database executions due to agnostic of database and the system manages same ease of understanding, dependability, and flexibility to that of actual cloud database as it does not need any intermediary server. It is customized towards cloud platforms and does not set up any intermediary proxy among client and cloud contributor. Proposed solution make itself differ from others because it does not have a need of usage of various cloud providers, and uses encryption algorithms to support regular SQL operations above encrypted information. The proposed strategy moves away from traditional methods that store data and save metadata in client machine. In the situation where several clients access similar database at the same time, the earlier works are rather ineffective. The data that is managed by protective database service comprises of metadata, encrypted metadata and as well as plaintext data. Plaintext data comprises of data that a tenant needs to store up and practice slightly in cloud database. For prevention of undependable cloud provider from violation of data privacy of tenant that is of plain form, protective database service make utilization of numerous methods of cryptography for changing of plaintext data to

encrypted tenant data for the reason that names of tables and columns have to be encrypted.

III. AN OVERVIEW OF PROPOSED SYSTEM

Insertion of important data in cloud provider has to assure security and ease of understanding for data in use. We implement a protective database service that acts as foremost solution allowing cloud tenant to gain various features such as ease of understanding, dependability, and flexibility devoid of revealing of unencrypted data towards cloud provider.

This protective database put together cloud services by means of data privacy as well as choice of synchronized operations on encrypted information [4]. Protective system is valid to any of the database systems as it does not modify services of cloud database. The solution manages distributed clients for connecting towards an encrypted database, and for implementation of autonomous operations. The database service secures data privacy by permitting of cloud server to perform concurrent operations above encrypted information. The proposed system has an improvement of eliminating intermediate proxies that limits to expediency dependability, and flexibility properties that are basically important in cloud solutions. Projected solution make itself differ from others because it does not have a need of usage of various cloud providers, and uses encryption algorithms to support regular operations above encrypted information. The proposed strategy moves away from traditional methods that store data and save metadata in client machine. In the situation where several clients access similar database at the same time, the earlier works are rather unsuccessful. Protective database service is compatible with standard database engines, and permits cloud tenant to gain various features to make a protective database service by means of controlling of cloud data services that are already existed. Proposed database service is suited with relational database servers, and it is compatible to several database executions due to agnostic of database and the system manages same ease of understanding, dependability, and flexibility to that of actual cloud database as it does not need any intermediary server. Proposed system associates more close to the works that makes use of encryption for protection of data that is manageable by undependable databases. Unlike advanced methods, proposed strategy does not depend on intermediary proxy that considers breakdown and blockage that confines accessibility of representative cloud services. Proposed strategy is customized towards cloud platforms and does not set up any intermediary proxy among client and cloud contributor. Exclusion of reliable intermediate server permits protective system to accomplish ease of understanding, dependability, and flexibility levels of cloud database. Proposed database service does not necessitate alterations to cloud database, and it is instantly appropriate towards existing cloud databases. Protective system clients get back needed metadata from untrustworthy database with the intention that numerous instances of client have permission towards undependable cloud database separately with assurance of similar ease of use as well as scalability properties [5][6]. Protective system clients generate set of metadata that consist of information necessary to encrypt as well as decrypt data in addition to management information. Workloads that comprise alterations towards database structure are managed by proposed system but at overheads that attain needed points of data privacy.

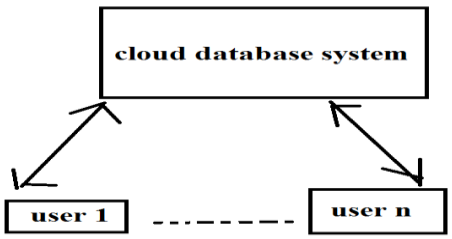

Fig1: an overview of proposed system.

IV. CONCLUSION

There are works that make sure protection of storage service privacy but protecting privacy in database services is an interesting area of study. In our work we apply a protective database service that acts as principal solution allowing cloud tenant to gain various features such as ease of understanding, dependability, and flexibility devoid of revealing of unencrypted data towards cloud provider. Protecting database service is well-suited with criterion database engines, and permits cloud tenant to gain various features to make a protective database service by means of controlling of cloud data services that are already existed. The database function that was projected secures data privacy by permitting of cloud server to perform concurrent operations above encrypted information. Prohibiting of consistent intermediate server permits protective system to accomplish ease of understanding and flexibility levels of cloud database. Protecting system clients produce set of metadata that consist of information necessary to encrypt as well as decrypt data in addition to management information.

V. REFERENCES

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

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

[3] 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.

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

[5] 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.

[6] 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.

