Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases

Abstract:

Placing critical data in the hands of a cloud provider should come with the guarantee of security and availability for data at rest, in motion, and in use. Several alternatives exist for storage services, while data confidentiality solutions for the database as a service paradigm are still immature. We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions. The efficacy of the proposed architecture is evaluated through theoretical analyses and extensive experimental results based on a prototype implementation subject to the TPC-C standard benchmark for different numbers of clients and network latencies.

Existing System:

Original plain data must be accessible only by trusted parties that donot include cloud providers,intermediaries and internet.in any untrusted context,data must be encrypted.Satisfying these goals has different levels of complexity depending upon the type of cloud service. These are several solutions ensuring confidentially for the storage as a service paradigm, while guaranteeing confidentially in the database as a service paradigm is still in an open research area.
DisAdvantages:

Can not apply fully homomorphic encryption schemes because of their excessive computational complexity.

Proposed System:

We propose a novel architecture that integrates cloud database services with data confidentially and the possibility of executing the concurrent operation on encrypted data.

This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database and to execute concurrent and independent operation including those modifying the database structure.

Secure Dbaas provides several original features that differentiate it from previous work in the field of security for remote database services.

Advantages:

The Proposed Architecture doesnot require modifications to the cloud database and it is immediately applicable to existing cloud dbaas.such as the experimented postgresQL plus cloud database,Windows Azure and Xeround.

There are no theoretical and practical limits to extend our solutions to other platforms and to include new encryption algorithm.

It provides the same availability,elasticity, and scalability of the original cloud dbaas because it doesnot require any intermediate server.
System Requirements:

Hardware Requirements:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech.
- Ram: 512 Mb.

Software Requirements:

- Coding Language: C#.net, Asp.net
- IDE: VisualStudio 2010