Providing Consistent and Secure Access to Cloud Database

[1]Sanket Rameshwarrao Milke
[1]PG Scholar
[1]Computer Science & Engineering Department
[1]Government Engineering College, Aurangabad, India

***Abstract* - Availability and scalability can be achieved by usual Cloud database services, but there is no guarantee about data confidentiality. Adding encryption with SQL operations is a favorable way although it is considered by many issues. Existing applications based on some trusted intermediate server adds limitations to availability and scalability of original cloud database services. We intend an architecture that avoids any intermediary component, thus achieving availability and scalability comparable to that of unencrypted cloud database services. Also our architecture promises data consistency in situations in which independent clients concurrently execute SQL queries, and the structure of the database can be modified. Several alternatives exist for storage services, while data confidentiality solutions for the database as a service model are still immature. We intend an architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. This is the 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 additional advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions.**

***IndexTerms* - Cloud, security, confidentiality, SecureDBaaS, database**

I. Introduction

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service(SaaS). We can call cloud The datacenter hardware and software together. When a cloud is made available in a pay-as-you-go manner to the general public , we call it Public Cloud and the service being sold is Utility Computing. Private Cloud refers to the internal datacenters of a business or other organization, not made available to the general public. So we can call Cloud Computing to the Software as a Service(SaaS) and Utility Computing together but excluding Private Clouds.

Cloud Computing, the long-held dream of computing as a utility, has the potential to change a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT.As a result, Cloud Computing is a popular topic for blogging and white papers and been featured in the title of workshops, conferences, and even magazines.

II. Related Work

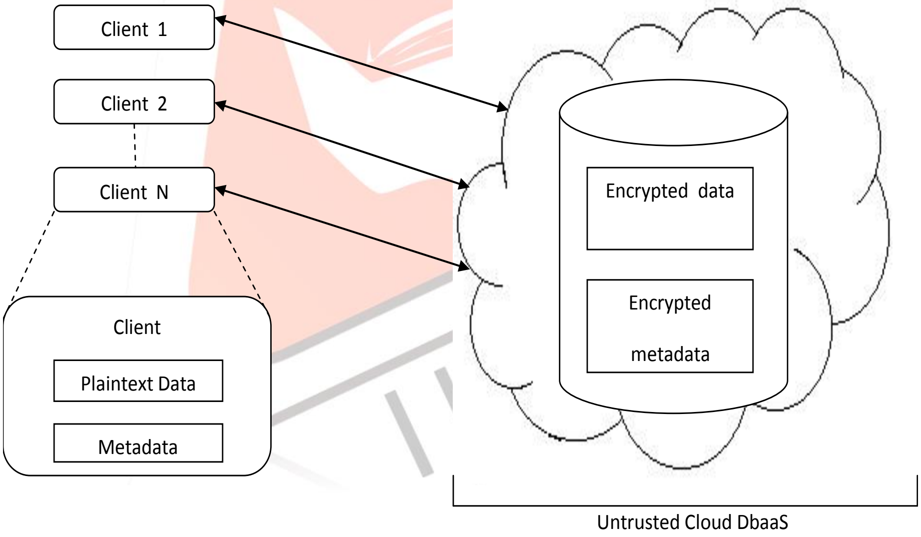
This paper intends an architecture that is different from previous work in the field of secure cloud database services. Cryptographic file systems and secure storage solutions represent the earliest works to provide confidentiality and integrity of data outsourced to untrusted cloud storage services. We do not detail the several papers and products in this field (e.g., [6, 10, 11]) because they do not allow any computation on encrypted data. Hence they cannot be applied to the context of cloud DBaaS. Some DBMS engines offer the possibility of encrypting data at the file system level through the so called Transparent Data Encryption (TDE) feature [3, 12]. This feature makes it possible to build a trusted DBMS over untrusted storage. However, in the DBaaS context the DBMS engine is not trusted because it is controlled by the cloud provider, hence the TDE approach is not applicable to cloud database services.

An approach to preserve data confidentiality in scenarios where the DBMS is not trusted is proposed in [5]. However it requires a modified DBMS engine that is not compatible with commercial and open source DBMS software adopted by cloud providers. On the other hand, the architecture we propose is compatible with standard DBMS engines, and allows customers to build a secure cloud database by leveraging cloud DBaaS readily available. Supporting Security and Consistency for Cloud Database 181 The proposal in [4] uses encryption to control accesses to encrypted data stored in a cloud database. This solution is not applicable to usage contexts in which the structure of the database changes, and does not support concurrent accesses from multiple clients possibly distributed on a geographical scale.

Data outsourcing or database as a service is a new model for data management in which a third party service provider hosts a database as a service. The service provides data management for its customers and thus obviates the need for the service user to purchase expensive hardware and software, deal with software upgrades and hire professionals for administrative and maintenance tasks. Since using an external database service promises reliable data storage at a low cost it is very attractive for companies. Such a service would also provide universal access, through the Internet to private data stored at reliable and secure sites. However, recent governmental legislations, competition among companies, and database thefts mandate companies to use secure and privacy preserving data management techniques. The data provider, therefore, needs to guarantee that the data is secure, be able to execute queries on the data, and the results of the queries must also be secure and not visible to the data provider. Current research has been focused only on how to index and query encrypted data. However, querying encrypted data is computationally very expensive. *Providing an efficient trust mechanism* to push both database service providers and clients to behave honestly has emerged as one of the most important problem before data outsourcing to become a viable model. In this paper, we describe scalable privacy preserving algorithms for data outsourcing. Instead of encryption, which is computationally expensive, we use distribution on multiple data provider sites and information theoretically proven secret sharing algorithms as the basis for privacy preserving outsourcing. The technical contributions of this paper is the establishment and development of a framework for efficient fault-tolerant scalable and theoretically secure privacy preserving data outsourcing that supports a diversity of database operations executed on different types of data, which can even leverage publicly available data sets.

III. Proposed System

Our proposal is related to [8] and [13] that preserve data confidentiality in an untrusted DBMS through encryption techniques that allow the execution of SQL queries over encrypted data and are compatible with common DBMS engines. These architectures are based on an intermediate and trusted proxy that mediates all the interactions between clients and the untrusted DBMS server. The reliance on a trusted proxy that characterizes both [8] and [13] facilitates the implementation of a secure DBaaS, but causes several drawbacks. A detailed comparison between the proxy-less architecture proposed in this paper and previous architectures based on a trusted proxy is in Section 3. The architecture we propose moves away from existing solutions because it allows multiple and independent clients to connect directly to the untrusted cloud DBaaS without any intermediate server. To the best of our knowledge this is the first paper that identifies consistency issues related to concurrent execution of queries over encrypted data and to propose viable solutions for different usage contexts, including data manipulation, modification to the database structure, and data re-encryption.



Our proposal provide security to the metadata in all conditions whether it is in rest, in motion or in use by the stored encrypted metadata at the cloud. Only clients knowing encryption key can decrypt metadata. In the intended architecture the plaintext database is converted into encrypted database by translating each plaintext table into corresponding encrypted table. Each encrypted table is associated with a set of metadata containing essential information to manage the encryption and decryption of data belonging to that table. Metadata associated with different tables are independent.

References

[1] M. Armbrust et al., “A View of Cloud Computing” Comm. Of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2] W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing.” Technical Report Special Publication 800-144, NIST, 2011.

[3] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, “SPORC: Group Collaboration using Untrusted Cloud Resources,” Proc. Ninth USENIX conf. Operating Systems Design and Implementation, Oct.2010.

[4] R.A. Popa, C.M.S. Redfield, N. Zeldovich and H. Balkrishnan, “CryptDB: Protected Confidentiality With Encrypted Query Processing,” Proc. ACM 23rd Symp Operating System Principles, Oct 2011.

[5] H. Hacigumus, B. Iyer, C. Li and S. Mehrotra, “Executing SQL Over Encrypteed Data in the Database-Service-Provider Model,” Proc. ACM SIGMOD Int’l Conf. management data, June 2002.

[6] E. Damiani, S.D.C. Vimercati, S. Jajodiya, S. Paraboschi, P. Samarati, “Balancing Confidentiality and Efficiency in Untrusted Relational dbms,” Proc Tenth ACM Conf. Computer and Comm. Security, Oct. 2003.

[7] 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.