ISSN 2395-1621

Security Challenges in Cloud Computing Infrastructures

[#1]Tehseen Shaikh, [#2]Aishwarya Shingare, [#3]Pooja Dhere, [#4]Prof. Y K. Patil

[1]shaikhtehseen904@gmail.com
[2]aishaishwarya60@gmail.com
[3]poojadhere271994@gmail.com

[#123]Department of Computer Engineering

[#4]Prof. Department of Computer Engineering

Bhivarabai Sawant Institute Of Technology Research
Wagholi, Pune.

ABSTRACT

In this we placed critical data in the hands of a cloud provide security and availability for data at rest and in use. Several alternatives exist for storage services, while data confidentiality solutions for the Database as a Service paradigm are still immature. A novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data .The first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and execute concurrent and independent operations which includes modifying the database structure .The further advantage of eliminating intermediate proxies that limit the elasticity, availability and scalability properties that are intrinsic in cloud-based solutions. The 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.

ARTICLE INFO

Article History

Received: 9th October 2015

Received in revised form :

10th October 2015

Accepted : 14th October 2015

Published online :

15th October 2015

Keywords: **Cloud Computing, SecureDBaaS, Encryption, Security,Database.**

I. INTRODUCTION

As there are number of critical data which is placed in some infrastructure of untrusted parties, we need some assurance about the privacy and security of data. Original data must be only accessible by trusted parties. There is different level of complexities while providing this confidentiality trusted to them. In this, we propose a new database which is secure (SecureDBaaS) as a first solution that allows cloud tenants to take full advantage of database qualities like availability, reliability, elasticity and scalability. This architecture is motivated to allow multiple, independent and geographically distributed clients to execute concurrent operations on encrypted data. This cloud provides database service, which includes SQL statements that modify the database structure to preserve the data confidentiality at the client and cloud level. Unlike SecureDBaaS, architectures relying on trusted intermediate proxy do not support the most typical cloud scenario where geographically dispersed clients can concurrently issue read/write operations and data structure modifications to a cloud database. SecureDBaas is immediately applicable to any DBMS because it requires no modification to the cloud database services. Workloads including modifications to the database structure are also supported by SecureDBaaS. The motivation of these results is that network latencies, which are typically of cloud scenarios, tend to mask the performance cost of data encryption on response time. The overall conclusion of this system is important because for the first time it demonstrates the applicability of encryption to cloud database services in the terms of feasibility and performance.

II. LITERATURE SURVEY

A view of cloud computing is an existing base paper which was proposed by author M. Armbrust et al. This paper was published in year 2010. In a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality is of paramount importance.

Guidelines on Security and Privacy in Public Cloud Computing are an existing base paper which was proposed by W. Jansen and T. Grance in the year 2011. In a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality is of paramount importance.

SPORC:Group Collaboration Using Untrusted Cloud Resources is an existing base paper which was proposed by author A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W.

Felten in the year 2010. The original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries, and Internet, in any untrusted context, data must be encrypted. Satisfying these goals has different levels of complexity depending on the type of cloud service.

Fully Homomorphic Encryption Using Ideal Lattices is an existing base paper which was proposed by author C. Gentry in the year 2009. This paper contains a theoretical discussion about solutions for data consistency issues due to concurrent and independent client accesses to encrypted data. In this context, we cannot apply fully homomorphic encryption schemes.

CryptDB: Protecting Confidentiality with Encrypted Query Processing is an existing base paper which was proposed by R.A. Popa, C.M.S Redfield, N. Zeldovich and H. Balakrishnan in the year 2011. This system was based on intermediate servers which was considered to be impractical for a cloud-based solution because any proxy represents a single point of failure and a system bottleneck that limits the main benefits(scalability, availability and elasticity) of a database service deployed on a cloud platform.

III.EXISTING SYSTEM

In a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality is of paramount importance. This requirement imposes clear data management choices: original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries, Internet; in any untrusted context data must be encrypted. Satisfying these goals has different levels of complexity depending on the type of cloud service. There are several solutions ensuring confidentiality for the storage as a service paradigm, while guaranteeing confidentiality in the database as a service (DBaaS) paradigm is still an open research area.

Issues of Existing System

- It is not secure.
- Satisfying these goals has different levels of complexity depending on the type of cloud service.
- We cannot apply fully homomorphic encryption schemes.
- The systems were based on intermediate servers which were considered to be impractical for a cloud-based solution because any proxy represents a single point of failure and a system bottleneck that limits the main benefits of a database service deployed on a cloud platform.
- Scalability, Availability and Elasticity was not provided.

IV. OBJECTIVE

To guarantee data confidentiality by allowing cloud database server to execute concurrent SQL operations over encrypted data.

To provide the same availability, elasticity and scalability of the original cloud DBaaS because it does not require any intermediate server.

Multiple clients, possibly geographically distributed, can access concurrently and independently a cloud database service.

To allow any party to access the data since the data is already in the encrypted form.

To provide compatibility with any relational database servers and to be applicable to any DBMS implementations.

To take advantage of secret sharing.

V. PROPOSED SYSTEM

The architecture design was motivated by a threefold goal: to allow multiple, independent, and geographically distributed clients to execute concurrent operations on encrypted data, including SQL statements that modify the database structure; to preserve data confidentiality and consistency at the client and cloud level; to eliminate any intermediate server between the cloud client and the cloud provider. The possibility of combining availability, elasticity, and scalability of a typical cloud DBaaS with data confidentiality are demonstrated through a prototype of SecureDBaaS that supports the execution of concurrent and independent operations to the remote encrypted database from many geographically distributed clients as in any unencrypted DBaaS setup. To achieve these goals, SecureDBaaS integrates existing cryptographic schemes, isolation mechanisms, and novel strategies for management of encrypted metadata on the untrusted cloud database. This paper contains a theoretical discussion about solutions for data consistency issues due to concurrent and independent client accesses to encrypted data. In this context, we cannot apply fully homomorphic encryption schemes because of their excessive computational complexity.

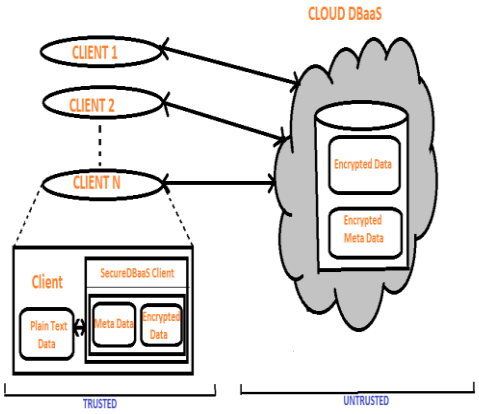

Fig 1: SecureDBaaS Architecture

Advantages of Proposed System

- The motivation of these results is that network latencies, which are typical of cloud scenarios, tend to mask the performance costs of data encryption on response time.
- SecureDBaaS is immediately applicable to any DBMS because it requires no modification to the cloud database services.
- Guarantees data confidentiality by allowing cloud database server to execute concurrent SQL operations over encrypted data.
- Multiple clients, possibly geographically distributed, can access concurrently and independently a cloud database service.
- To allow any party to access the data since the data is already in the encrypted form.
- To provide compatibility with any relational database servers and to be applicable to any DBMS implementations.
- Secret sharing.

VI. CONCLUSION

This system proposes an innovative architecture that guarantees confidentiality of data stored in public cloud databases. The solution of the system does not rely on intermediate proxy that we consider a single point of failure and a bottleneck limiting availability and scalability of typical cloud database services. It supports concurrent SQL operations on encrypted data issued by heterogenous and possibly geographic dispersed clients. It is immediately applicable to existing cloud DBaaS. These performance results open the space for future improvements that we are investigating.

REFERENCE

[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] J. Li, M. Krohn, D. Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth USENIX Conf. Operating Systems Design and Implementation, Oct. 2004.

[4] 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.

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

[6] 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.

[7] 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, June2002.

[8] 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.

[9] E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, July/Aug. 2006.

[10] D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, "Database Management as a Service: Challenges and Opportunities," Proc. 25th IEEE Int'l Conf. Data Eng., Mar.-Apr. 2009.

[11] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani, "Distributing Data for Secure Database Services," Proc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.

