ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Secure Access to Encrypted Cloud Database

Chandan M N, Prof. Divakar H.R

PG Scholar, Department of MCA, PES College of Engineering, Mandya (d), Karnataka, India

Assistant Professor, Department of MCA, PES College of Engineering, Mandya (d), Karnataka, India

ABSTRACT: Cloud computing is one of the most increasing one with the increase number of cloud users. In today's environment every user wants to access their data at any time and at anywhere. In an organization they store their data only on their computers, if they want their data during roaming situation means it is not possible one to carry the data at every time, this is a difficult factors for an organization. Cloud computing can address this problem by providing data storage mechanism to access the data at anywhere. This is one of the storage device used to access their data at anywhere through networks which is called cloud provider. For this service user worry about the security and privacy issue under this cloud computing for their personal data. For this issue this survey shows various techniques for the security and privacy mechanism for the user data. There are many data storage techniques available, but we are trying to combine cloud database service along with data security and also can perform independent and concurrent operations on encrypted data.

KEYWORDS: - Cloud Storage, Security, Independent Access, DBaaS.

I.INTRODUCTION

The cloud computing paradigm is successfully come together as the fifth utility, but this positive trend is in part limited by concerns of information confidentiality and unclear costs over a medium-long term .We are interested in the database as a service standard that poses many research challenges in terms of security and cost evaluation from a tenant's point of view. Most results regarding encryption for cloud-based services are not capable of being applied to the database paradigm. Other encryption schemes that are used in the execution of SQL operations over encrypted data either have limits in their performance or require the choice of which encryption scheme must be adopted for each database column and SQL operation. These latter proposals are fine when the set of queries can be determined in a static manner at design time, while we are involved in other common outline where the workload might change after the data- base design. In this paper, we propose a novel architecture for adaptive encryption of public cloud databases that offers a proxy-free alternative to the system represented. The proposed architecture will meet certain specifications in an adaptive way the best level of data confidentiality for any database workload, even when the set of SQL queries changes dynamically.

The cloud can hold the user liable to account for one's action for the data it outsources, and similarly, the cloud is itself reasonable for the services it provides. The user's validity who stores the data is also verified. Other than the technical solutions to ensure security and privacy, there is also a need for the observance of law. Access control is gaining importance because it is important that only authorized users have access to valid service in clouds.

A huge amount of sensitive information is being stored in the cloud. Care should be taken to ensure access control of sensitive information which can often be related to health issues, confidential documents or even personal information as in social networking. The use of fully homomorphism encryption would guarantee the execution of any operation over encrypted data, but existing implementations are affected by huge computational costs to the extent that the execution of SQL operations over a cloud database would become speculative.

II.RELATED WORK

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

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.

III.LITERATURE SURVEY

In the database world, the enterprise data management world, when enterprises found out the need to create data warehouses to gather their historical business data and to run relational queries over that data for the purpose of reporting and analysis of business, big data problems arose. Efficient analysis and storage of such data on ―database machines‖ that could be dedicated to such purposes. The database machines earlier involved a mixed recommendations of novel hardware architectures and designs for prehistoric parallel query processing techniques. Within a few years it became clear that neither brute force scan-based parallelism nor proprietary hardware would become reasonable substitutes for good algorithms and software data structures. This clear understanding led to the first generation of software-based parallel databases based on the architecture now commonly referred to as ―shared-nothing‖. As the name implies the architecture of a shared nothing parallel database system, is based on the use of a networked cluster of Individual machines each with their own private processors, main memories, and disks. All data communications and inter-machine coordination is accomplished via message passing. These systems exploited the declarative, set-oriented nature of relational query languages and pioneered the use of divide and-conquer parallelism based on hashing in order to partition data for storage as well as relational operator execution for query processing Cryptographic approaches and usage policy rules must be considered. When someone wants to access data, the system should check its policy rules and reveal it only if the policies are satisfied. Existing cryptographic techniques can be utilized for data security, but privacy protection and outsourced computation need significant attention—both are relatively new research directions. Data provenance issues have just begun to be addressed in the literature. In some cases, information related to a particular hardware component (storage, processing, or communication) must be associated with a piece of data. Although security and privacy services in the cloud can be fine-tuned and managed by experienced groups that can potentially provide efficient security management and threat assessment services, the issues we've discussed here show that existing security and privacy solutions must be critically reevaluated with regard to their appropriateness for clouds.

IV.PROPOSED SYSTEM

The proposed architecture does not 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 solution to other platforms and to include new encryption algorithm. It guarantees data confidentiality by allowing a cloud database server to execute concurrent SQL operations (not only read/write, but also modifications to the database structure) over encrypted data. It provides the same availability, elasticity, and scalability of the original cloud DBaaS because it does not require any intermediate server.
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. Secure DBaaS provides several original features that differentiate it from previous work in the field of security for remote database services

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

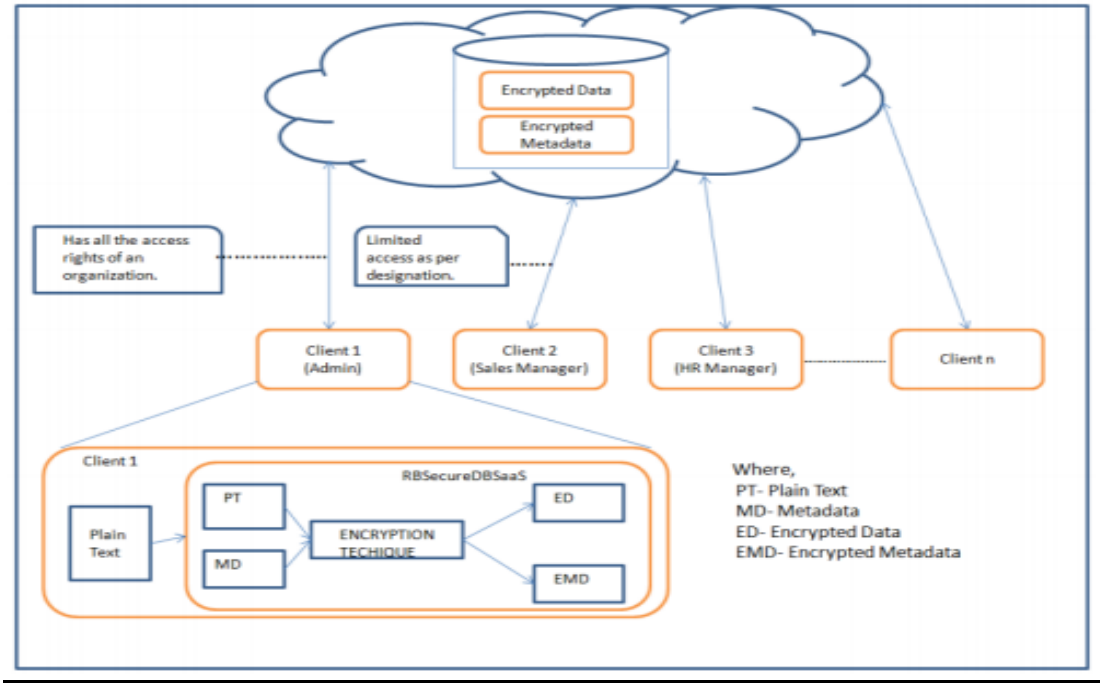
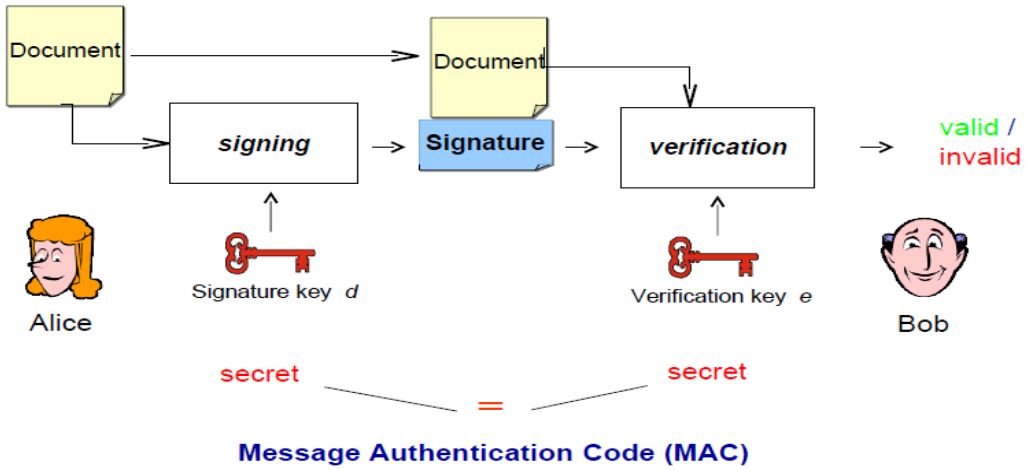


Fig. 2.1 SYSTEM ARCHITECTURE

MESSAGE AUTHENTICATION CODE (MAC)

Authenticity, integrity
Electronic Signature (= asymmetric signature)
Authenticity, integrity, non-repudiation
Encryption: Confidentiality
Encryption: $c \equiv m^e \bmod n$ (m is the plaintext)
Decryption: $m \equiv c^d \bmod n$ (c is the cipher text)



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V.EXPERIMENTAL RESULTS

We demonstrate the applicability of Secure DBaaS to different cloud DBaaS solutions by implementing and handling encrypted database operations on emulated and real cloud infrastructures. The present version of the Secure DBaaS prototype supports Postgre SQL, My Sql, and SQL Server relational databases. As a first result, we can observe that porting Secure DBaaS to different DBMS required minor changes related to the database connector, and minimal modifications of the codebase. We refer to Appendix C, available in the online supplemental material, for an in-depth description of the prototype implementation. Other tests are oriented to verify the functionality of Secure DBaaS on different cloud database providers. Experiments are carried out in Xeround, Postgres plus Cloud Database, Windows SQL Azure, and also on an IaaS provider, such as Amazon EC2, that requires a manual setup of the database. The first group of cloud providers offers ready-to-use solutions to tenants, but they do not allow a full access to the database system. For example, Xeround provides a standard My Sql interface and proprietary APIs that simplify scalability and availability of the cloud database, but do not allow a direct access to the machine.

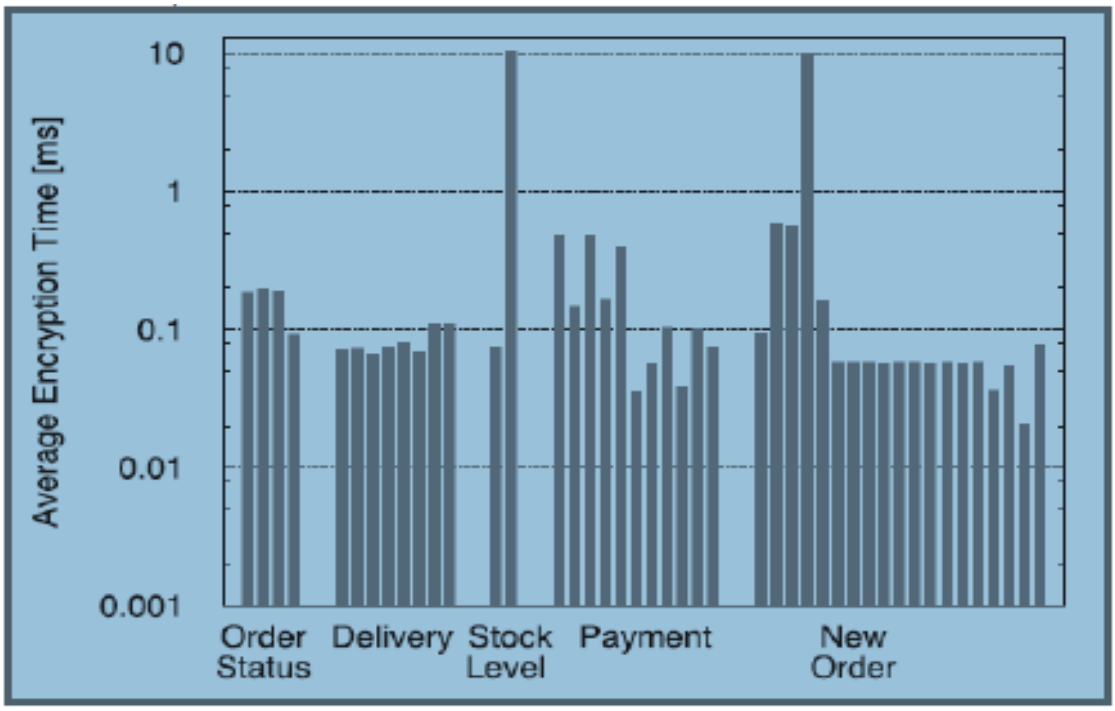


Fig 1 :Encryption times of TPC-C benchmark operations grouped by the transaction class

This prevents the installation of additional software, the use of tools, and any customization. On the positive side, SecureDBaaS using just standard SQL commands can encrypt tenant data on any cloud database service. Some advanced computation on encrypted data may require the installation of custom libraries on the cloud infrastructure. This is the case of Postgres plus Cloud that provides SSH access to enrich the database with additional functions. The next set of experiments evaluates the performance and the overheads of our prototype. We use the Emulab test bed that provides us a controlled environment with several machines, ensuring repeatability of the experiments for the variety of scenarios to consider in terms of workload models, number of clients, and network latencies. As the workload model for the database, we refer to the TPC-C benchmark. The DBMS server is PostgreSQL9.1 deployed on a quad-core Xeon having 12 GB of RAM. Clients are connected to the server through a LAN, where we can introduce arbitrary network latencies to emulate.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

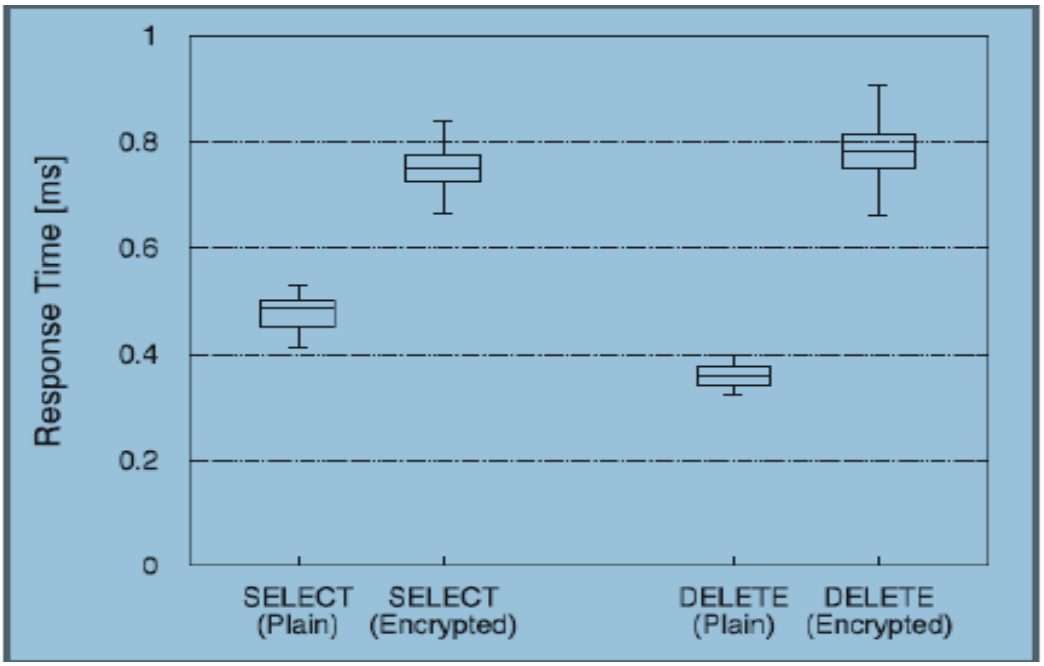


Fig 2: Plain versus encrypted SELECT and DELETE operations

WAN connections that are typical of cloud services the experiments evaluate the overhead of encryption, compare the response times of plain versus encrypted database operations, and analyze the impact of network latency. We consider two TPC-C compliant databases with 10 warehouses that contain the same number of tuples: plain tuples consist of 1,046 MB data, while SecureDBaaS tuples have size equal to 2,615 MB because of encryption overhead. Both databases use repeatable read (snapshot) isolation level. In the first set of experiments, we evaluate the overhead introduced when one SecureDBaaS client executes SQL operations on the encrypted database. Client and database server are connected through a LAN where no network latency is added. To evaluate encryption costs, the client measures the execution time of the 44 SQL commands of the TPC-C benchmark. Encryption times are reported in the histogram of that logarithmic Y -axis.

VI.CONCLUSION

In this paper we have discuss about the distributed database system that is considered to be more reliable than centralized database system. We also describe the concurrency control algorithms-: distributed 2PL, wound-wait, basic timestamp ordering and distributed optimistic algorithm. It is real important for database to have the ACID properties to perform.

VII.FUTURE SCOPE

The transaction is assigned a globally unique timestamp. This time stamp is sent to each cohort in the "prepare to commit" message, and it is used to locally certify all of its reads and writes as follows : A read request is certified if-:
(i) The version that was read is still the current version of the item, and
(ii) No write with a newer timestamp has already been locally certified. A write request is certified if-:
(i) No later reads have been certified and subsequently committed, and
(ii) No later reads have been locally certified already

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

REFERENCES

[1] Gupta V.K., Sheetlani Jitendra, Gupta Dhiraj and Shukla Brahma Datta, Concurrency control and Security issues in Distributed database system, Vol. 1(2),70-73, August (2012)
[2] Arun Kumar Yadav& Ajay Agarwal, An Approach for Concurrency Control in Distributed Database System, Vol. 1, No. 1, pp. 137-141, January-June (2010)
[3] Navathe Elmasri, Database Concepts, Pearson Education, V edition (2008)
[4] Fundamentals of DBMS, Lakhanpal Publisher, III edition (2008)
[5] Swati Gupta, Kuntal Saroha, Bhawna, Fundamental Research of Distributed Database, IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 02, Aug 2011
[6]DistributedDatabase: http://wps.pearsoned.co.uk/wps/media/objects/10977/11240737/Web%20chapters/Chapter%2012_WEB.pdf

[7]. Amazon elastic compute cloud (Amazon EC2), http://aws.amazon.com/ec2/.
[8]. Hacigumus, B. Iyer, and S. Mehrotra, "Providing Database as aService" Proc. 18th IEEE Int'l Conf. Data Eng., Feb. 2002.
[9]. J. Li, M.Krohn, D.Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)" Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation, Oct. 2004.
[10]. 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.
[11]. E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model" Proc. 20th Ann. IFIP WG 11.3Working Conf. Data and Applications Security, July/Aug. 2006.
[12]. 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.

BIOGRAPHY

Chandan M N is a PG Scholar in MCA , PES College of Engineering, Mandya VTU University, Karnataka. He is pursuing Master of Computer Application (MCA) degree 2017.

Prof .Divakar H R Assistant Professor, Department of MCA, PES College of Engineering, Mandya (d), Karnataka, India