ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cryptography Schemes for Accessing Distributed, Concurrent & Independent Encrypted Cloud Information

K.Chaitanya Lakshmi
M.Tech Student,
Department of CSE,
Vignan's Nirula Institute of Technology and Science for Women.

M.Vasumathi Devi, Ph.D
Assistant Professor,
Department of CSE,
Vignan's Nirula Institute of Technology and Science for Women.

Abstract:

Cloud information environments square measure terribly enticing for the readying of huge scale applications attributable to their extremely ascendible and offered infrastructure. information as a Service (DBaaS) model is employed to manage databases in cloud setting. Secure DBaaS standardprovides information confidentiality for cloud storage. Secure DBaaS is intended to permit multiple and freelance purchasers to attach to the cloud while not intermediate server.Files, information structures and information square measure encrypted before transfer to the cloud. Multiple cryptography techniques square measure wont to convert plain text into encrypted information. Table names and their column names also are encrypted within the cloud information safetytheme. The system supports geographically distributed purchasers to attach on to AN encrypted cloud information. during this paper we tend to quadrangularmeasure proposing new design that integrate cloud storage service with information privacy and possess a feature of corporal punishment co-occurring operations on encrypted information and together with the geographically distributed purchasers to attach on to these cloud information that is encrypted and that they conjointly provided to execute their operations over the cloud information. This design eliminates the brokers (Intermediate proxies) it limits the quantifiability, elasticity, accessibility. High sensitive information square measure encrypted by RSA cryptography and regular information square measure encrypted exploitation AES technique so overhead on the network will be reduced.

1. INTRODUCTION:

Cloud based mostly services have become common as they specialise in high accessibility and quantifiability at low value. whereas providing high accessibility and quantifiability, inserting essential knowledge to cloud poses several security problems. For avoiding these security problems the info area unit keep within the cloud information in associate encrypted format. The encrypted cloud information permits the execution of SQL operations by choosing the cryptography schemes that support SQL operators. Encrypted cloud information permits differing types of accesses like distributed, concurrent, and freelance. one in all the design that supports these 3 types of access is Secure DBaaS. The Secure DBaaS design supports multiple and freelance shoppers to execute synchronal SQL operations on encrypted knowledge. knowledge consistency ought to be maintained by investment concurrency management mechanisms utilized in database management system engines. This survey explains the assorted concurrency management protocols that may be utilized in the encrypted cloud information. The applications want 1SR if knowledge is replicated. Hence, to ensure the deserves of cloud, it\'s essential to produce high quantifiability, accessibility, low value and knowledge with sturdy consistency, that is ready to dynamically adapt to system conditions. Self optimizing one copy serializability (SO-1SR) is that the concurrency management protocol that dynamically optimizes all stages of dealing execution on replicated knowledge within the cloud information. Current DBMSs supported by cloud suppliers permits relaxed consistency guarantees that successively increase the look complexness ofrequests. The second concurrency controllingprotocol is that the pic isolation (SI) that provides redoubled concurrency in cloud atmosphere in comparison to 1SR. Transactions area unit browse from the pic, reads area unit never blocked attributable to write locks that successively will increase concurrency. SI doesn't permit several of the inconsistencies, SI permits dealing inversions. To avoid dealing inversions sturdy consistency guarantee is needed, i.e. sturdy SI (SSI). The third concurrency management protocol is that the session consistency (SC). Session consistency could be a completely different type of ultimate consistency. The system provides browse your writes consistency within every session. Session consistency is at a coffee value whereas considering interval and dealing value.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the value based mostly concurrency management within the cloud is that the C three i.e. cost-based adaptive concurrency management in cloud. C3 dynamically switch between sturdy consistency level and weak consistency level of transactions during a cloudinformation in line with the value at runtime. it\'s designed on the highest of 1SR and SSI.

2. SYSTEM ARCHITECTURE:

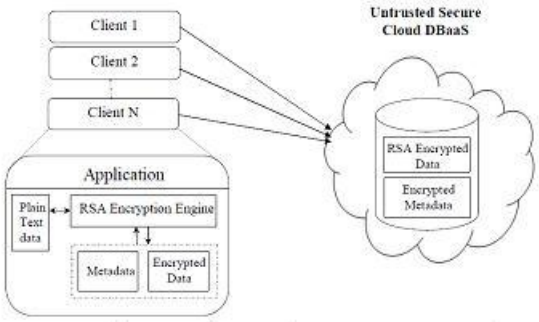


Fig 1: Architecture of Untrusted secure Encrypted Cloud Database.

The System has to reach different platforms and to incorporate new encoding algorithmic rule with untrusted cloud information and trustworthy proxy has to be removed. The virtual machine image on cloud uses cloud information severally. this will be achieved by victimization consumer application and cloud knowledgebase with RSA encoding engine for top security and AES encoding for normal data to quick access. The encrypted knowledge is keep into the untrusted cloud information with encrypted data. Clouds don\'t would like any trustworthy proxy for authentication and cloud information is genuine as untrusted.

EXISTING SYSTEM:

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. There are several solutions ensuring confidentiality for the storage as a service paradigm, while guaranteeing confidentiality in the database as aservice (DBaaS) paradigm is still an open research area.

DISADVANTAGES OF EXISTING SYSTEM:

Cannot 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 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.

ADVANTAGES OF PROPOSED SYSTEM:

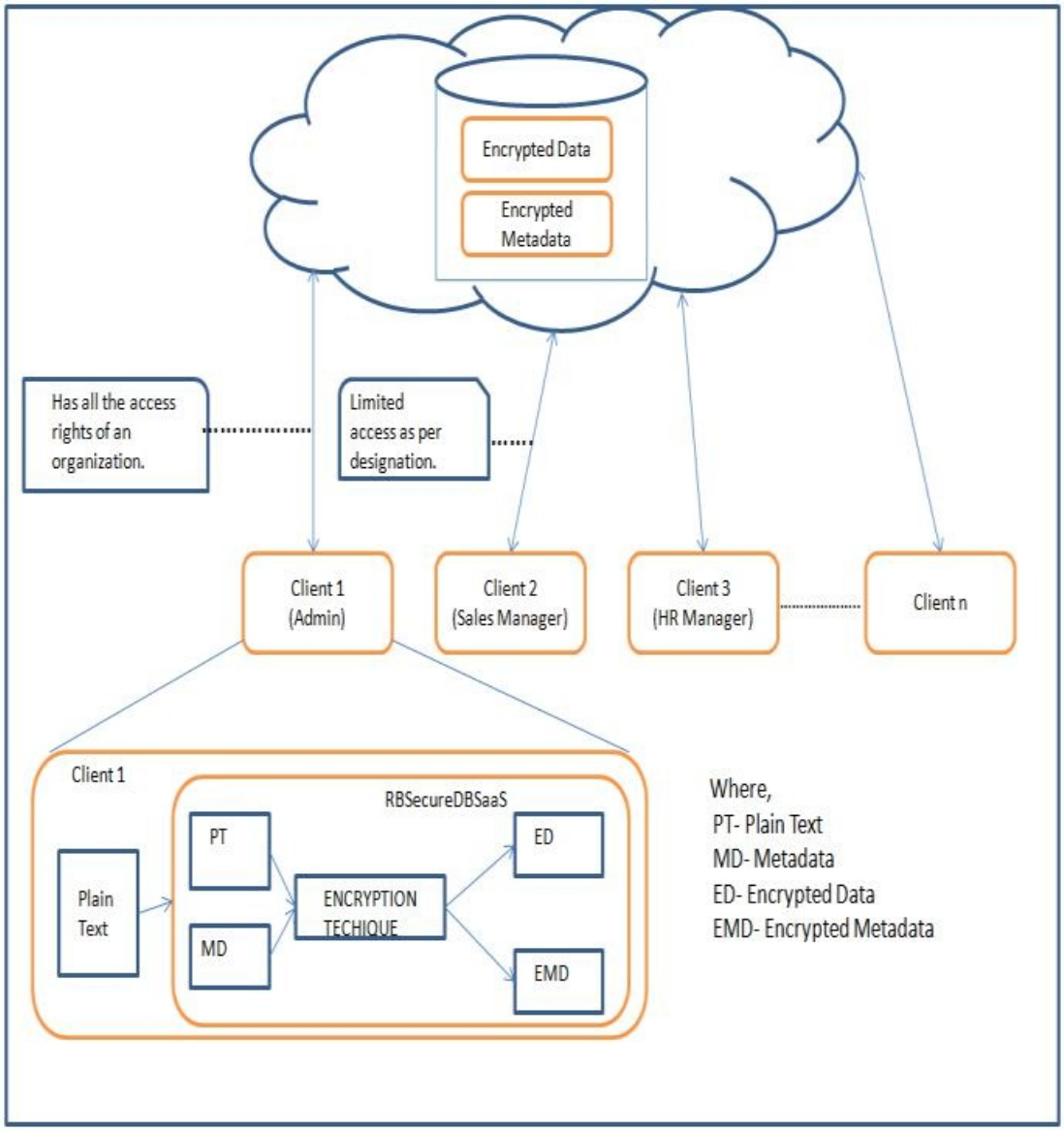
The proposed architecture does not require modifications to the cloud database, and it is immediately applicable to existing cloud DBaaS, such as the experimented PostgreSQL Plus Cloud Database, Windows Azure and Xeround .There are no theoretical and practical limits to extend our solution to other platforms 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2.1 MODULE DESCRIPTION:

2.1.1 N - consumer –



System module uses one to N consumer information user that is employed to write knowledge as RSA encoding. The JDBC accustomed connect with the cloud information. consumer information is verified and genuine before association to the cloud information.

2.1.2 Encrypted data –

The question author is that the computer code element that interprets plaintext commands processed by the operation computer program into SQL commands which will be dead by the untrusted cloud information over encrypted knowledge.

It leverages the encoding engine to execute all the encoding operations. Moreover, it interacts with the data manager to envision whether or not all the operators contained into the plaintext commands area unit supported by the encoding policies applied to the relevant tenant knowledge. Translated SQL commands area unit forwarded to the quality information connation.

2.1.3 Access to consumer –

SecureDBaaS proposes a unique approach wherever all knowledge and data area unit keep within the cloud information.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SecureDBaaS purchasers will retrieve the required data from the untrusted information through SQL statements, so multiple instances of the SecureDBaaS consumer will access to the untrusted cloud information severally with the guarantee of an equivalent handiness and measurability properties of run of the mill cloud DbaaS.

2.1.4 Verification and Authentication –

Client user will login secure cloud information solely when verification and Authentication for SQL execution like produce, Read, Update and delete knowledge from cloud information. RSA involves a public key and personal key. the general public key will be better-known to everybody, it\'s accustomed write messages. Messages encrypted victimization the general public key will solely be decrypted with the personal key. the general public secret\'s made from the modulus n and therefore the public (encryption) exponent e. The personal secret\'s made from the modulus n and therefore the personal (or decryption) exponent d that should be unbroken secret.

3.IMPLEMENTATION:
Metadata Management:

Metadata generated by SecureDBaaS contain all the data that\'s necessary to manage SQL statements over the encrypted info in an exceedingly means clear to the user. data management ways represent an artless plan as a result of SecureDBaaS is that the initial design storing all data within the untrusted cloud info along side the encrypted tenant information. SecureDBaaS uses 2 varieties of data. • info data area unit associated with the full info. there\'s only 1 instance of this data sort for every info. • Table data area unit related to one secure table. every table data contains all info that\'s necessary to cypher and decode information of the associated secure table.

This style selection makes it doable to spot that data sort is needed to execute any SQL statement so a SecureDBaaS consumer must fetch solely the data associated with the secure table/s that is/are concerned within the SQL statement. This style selection minimizes the quantity of data that every SecureDBaaS consumer has got to fetch from the untrusted cloud info, so reducing information measure consumption and interval. Moreover, it permits multiple purchasers to access severally data associated with completely different secure tables.

info data contain the cryptography keys that area unit used for the secure varieties. a special cryptography secret is related to all the doable combos of information sort and cryptography sort. Hence, the info data represent a hoop and don\'t contain any info concerning tenant information. The structure of a table data is portrayed in Fig. 3. Table data contain the name of the connected secure table and therefore the unencrypted name of the connected plaintext table. Moreover, table data embody column data for every column of the connected secure table.

4. CONCURRENT SQL OPERATIONS:

Support to the execution of SQL statements issued by multiple freelance (and presumptively geographically distributed) customers is one in each of the foremost necessary edges of SecureDBaaS with relevancy progressive solutions. Our style ought to guarantee consistency among encrypted tenant information and encrypted data as a results of corrupted or obsolete information would stop purchasers from cryptography encrypted tenant information resulting in permanent information losses. AN intensive analysis of the potential issues and solutions related to synchronic SQL operations on encrypted tenant information and information is contained in Appendix B, out there inside the on-line supplemental material. Here, we\'ve got an inclination to comment the importance of characteristic 2 classes of statements that square measure supported by SecureDBaaS: SQL operations not inflicting modifications to the knowledge structure, like browse, write, and update; operations involving alterations of the knowledge structure through creation, removal and modification of data tables. Here, we have got AN inclination to remark the importance of distinctive 2 categories of statements that unit supported by SecureDBaaS: SQL operations not inflicting modifications to the info structure, like scan, write, and update; operations involving alterations of the info structure through creation, removal, and modification of data tables (data definition layer operators). In eventualities defined by a static data structure, SecureDBaaS permits purchasers to issue synchronize SQL commands to the encrypted cloud data whereas not introducing any new consistency issues with relevancy unencrypted databases. once data retrieval, a noticeable text SQL command is translated into one SQL command operative on encrypted tenant information. As data doesn\'t would like modification, a consumer will browse them once and cache them for added uses successively thus rising performance.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SecureDBaaS is that the primary style that allow to synchronize and consistent accesses even once there area unit operations that will modify the knowledge structure. In such cases, we have got to make sure the consistency of data through isolation levels that we have a tendency to tend to demonstrate can work for several victimization eventualities

Experimental Results:

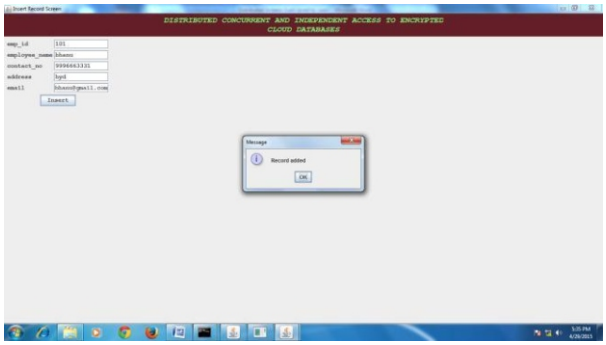


Fig 2. Inserting Employee details

After inserting the Employee details, these details will stored in database in encrypted format. In the below figure will show encrypted data and encrypted columns.

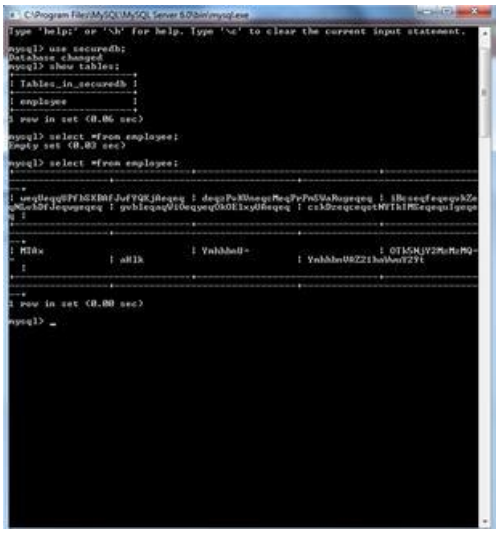


Fig 3: Storing Data in encrypted form.

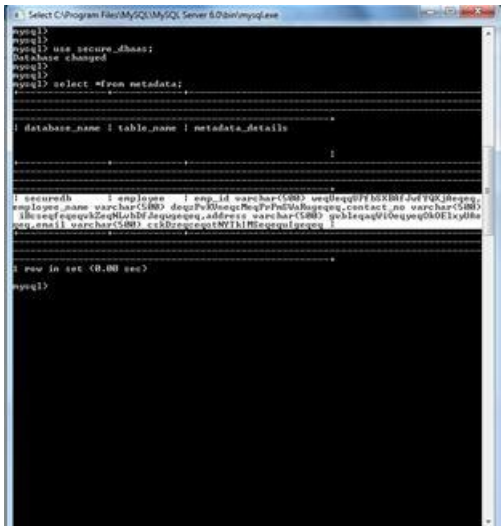


Fig 4: Meta data in the form of Encrypted data

Conclusion:

The paper proposes a novel solution that guarantees confidentiality of data saved into cloud databases that are untrusted by definition. All data outsourced to the cloud provider are encrypted through RSA and AES cryptographic algorithms that allow the execution of standard SQL queries on encrypted data. This is one of the solution that allows direct, independent and concurrentaccess to the cloud database and that supports even changes to the database structure. It does not rely on a trusted proxy that represents a single point of failure and a system bottleneck, and that limits the availability and scalability of cloud database services. Concurrent read and write operations that do not modify the structure of the encrypted database are supported.

There are various encryption decryption techniques available and are having their limitations. The architectural design in this paper uses RSA algorithm which is highly secure for data, but RSA encryption may increase overheads, therefore to decrease the overhead in the network. Very important data are encrypted using RSA and remaining data are encrypted using AES. Specifically, simultaneous read and compose operations that don't adjust the structure of the encoded database cause unimportant overhead. Dynamic situations described by simultaneous adjustments of the database structure are upheld, however at the cost of high computational expenses. These execution effects open the space to future changes are exploring.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

References:

[1]L. Ferretti, F. Pierazzi, M. Colajanni, and M. Marchetti, "Security and confidentiality solutions for public cloud database services," in SECURWARE2013, The Seventh International Conference on Emerging Security Information, Systems and Technologies, 2013, pp. 36–42.

[2]L. Ferretti, M. Colajanni, M. Marchetti, and A. E. Scaruffi, "Transparent Access on Encrypted Data Distributed over Multiple Cloud Infrastructures," in CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013, pp. 201–207.

[3]H. Hacigumu s, B. Iyer, and S. Mehrotra, Providing Database as a Service, Proc. 18th IEEE Intl Conf. Data Eng., Feb. 2002. [7] C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices, Proc.41st Ann. ACM Symp. Theory of Computing May 2009.

[4]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

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

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

[8]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.

[9] Efficient Method to Secure Web applications and Databases against SQL Injection Attacks, Zeinab Raveshi, Sonali R. Idate IJARCSSE Volume 3, Issue 5, May 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[10]Secured Data Storage in Google Cloud S.SABARI VASAN, I.GOLDA SELIA, International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue4 –April 2013.

[11]Handling Confidential Data on the Untrusted Cloud: An Agent-based Approach Ernesto Damiani, Francesco Pagano CLOUD COMPUTING 2010:International Conference on Cloud Computing, GRIDs, and Virtualization.