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

Appropriated Concurrent and Self adequate Clientele Access to Encrypted Impair Sources

Chilakapati Neelima
Department of Computer Science and Engineering
GIET Engineering College,
Rajamahendravaram, Andhra Pradesh - 533296, India.

K. Nagaraju
Department of Computer Science and Engineering
GIET Engineering College,
Rajamahendravaram, Andhra Pradesh - 533296, India.

Abstract

Putting imperative data in the hands of the haze up supplier must accompany the guarantee associated with solidness alongside openness expected for data with unwind, inside movement, alongside utilized. Various exchange choices are available expected for safety's sake organizations, while data attentiveness solutions for the vault to be a help worldview are in any case untimely. Every one of us offer the book structures that joins mist up store organizations alongside data prudence and furthermore the likelihood of making simultaneous surgical strategies with encoded data utilizing RSA Algorithm. This is really the primary arrangement advancing topographically spread customer base for interfacing on to an encoded mist up store, additionally to execute simultaneous alongside free surgical strategies, for example, people altering the vault development. The arranged structures gives the furthermore fortunate thing about killing further developed intermediaries that cutoff the suppleness, openness, alongside adaptability segments which may be inbuilt inside cloud-based cures. The proficiency on the arranged structures can be considered because of hypothetical examinations alongside generous test comes about relying upon the model execution subject to the TPC-C ordinary standard proposed for extraordinary quantities of customer base alongside group latencies.

INTRODUCTION

Cloud computing technology is a service-based, Internet-centric, safe, convenient data storage and network computing service. It is an internet-based model [1] for enabling a convenient and on-demand network access to a shared pool of configurable computing resources.

One of the important service of cloud computing is database as a service. Database-as-a-Service (DBaaS) [2] is a service that is managed by a cloud operator that supports applications, without the application team assuming responsibility for traditional database administration functions. With a DBaaS, the application developers should not need to be database experts, nor should they have to hire a database administrator (DBA) [3] to maintain the database.

True DBaaS will be achieved when application developers can simply call a database service and it works without even having to consider the database. The ultimate goal of a DBaaS is that the customer doesn't have to think about the database. Today, cloud users don't have to think about server instances, storage and networking, they just work. Virtualization enables clouds to provide these services to customers while automating much of the traditional pain of buying, installing, configuring and managing these capabilities.

Now database virtualization is doing the same thing for the cloud database and it is being provided as Database as a Service (DBaaS).

Cite this article as: Chilakapati Neelima & K. Nagaraju,"Appropriated Concurrent and Self adequate Clientele Access to Encrypted Impair Sources", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 4 Issue 12, 2017, Page 29-37.

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

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

On-demand self-service:

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access:

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) [4].

Resource pooling:

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines [5].

Rapid elasticity:

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

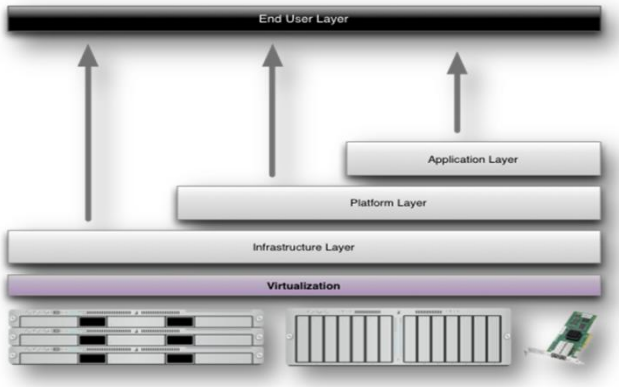
Measured service:

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Characteristics of cloud computing

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [6]. The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care



Structure of service models

Benefits of cloud computing:

- Achieve economies of scale.
- Reduce spending on technology infrastructure.
- Globalize your workforce on the cheap.
- Streamline processes.
- Reduce capital costs.

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

- Improve accessibility.
- Monitor projects more effectively.
- Less personnel training is needed.
- Minimize licensing new software.
- Improve flexibility.

PROBLEM STATEMENT:

The ever increasing demand for computing resources has led companies and resource providers to build large warehouse-sized data centers, which require a significant amount of power to be operated and hence consume a lot of energy. Cannot apply fully homomorphic encryption schemes because of their excessive computational complexity. Client and database server are connected through a LAN where no network latency is added.no key is used for encryption and decryption so it provides low security.

EXISTING SYSTEM

- 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.
- DBaaS provides several original features that differentiate it from previous work in the field of security for remote database services [7].

DISADVANTAGES OF EXISTING SYSTEM:

- Here in this system we cannot apply fully homomorphic encryption schemes because of their excessive computational complexity.

PROPOSED SYSTEM:

- The proposed architecture does not require modifications to the cloud database, and it is immediately applicable to existing cloud DBaaS.
- Initial option supporting geographically sent out customers to connect straight away to a encrypted foriegn data bank, also to implement concurrent along with self-sufficient businesses such as those people editing this data bank structure [8].
- We propose an enhanced algorithm like RSA algorithm to overcome the problem of homomorphic encryption schemes through which computational cost is reduced.
- In this paper we enhance security issues by adding a module that uses Gmail server to authenticate user by providing keys as mail to authorized user which is required to encrypt or decrypt the message to get key.

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 [9]
- Supporting geographically distributed clients to connect directly to an encrypted cloud database
- Execute concurrent and independent operations including those modifying the database structure
- 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.

MODULES:

1. Plain data Management
2. Metadata Management
3. Sequential Sql Operations
4. Concurrent Sql Operations

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

Modules Description:

Plain data Management:

Plaintext data consist of information that a tenant wants to store and process remotely in the cloud DBaaS. To prevent an untrusted cloud provider from violating confidentiality of tenant data stored in plain form, SecureDBaaS adopts multiple cryptographic techniques to transform plaintext data into encrypted tenant data and encrypted tenant data structures because even the names of the tables and of their columns must be encrypted. We describe how to initialize a SecureDBaaS architecture from a cloud database service acquired by a tenant from a cloud provider. We assume that the DBA creates the metadata storage table that at the beginning contains just the database metadata, and not the table metadata. The DBA populates the database metadata through the Secure DBaaS client by using randomly generated encryption keys for any combinations of data types and encryption types, and stores them in the metadata storage table after encryption through the master key. Then, the DBA distributes the master key to the legitimate users. User access control policies are administrated by the DBA through some standard data control language as in any unencrypted database. In the following steps, the DBA creates the tables of the encrypted database.

Data Management: It assumes that tenant data are saved in a relational database. It has to preserve the confidentiality of the stored data and even of the database structure because table and column names may yield information about saved data. This paper distinguishes the strategies for encrypting the database structures and the tenant data. Encrypted tenant data are stored through secure tables into the cloud database. To allow transparent execution of SQL statements, each Plaintext table is transformed into a secure table because the cloud database is untrusted. Secure DBaaS offers three field confidentiality attributes:

1) Column (COL) is the default confidentiality level that should be used when SQL statements operate on one column; the values of this column are encrypted

2) Multicolumn (MCOL) [10] should be used for columns referenced by join operators, foreign keys, and other operations involving two columns; the two columns are encrypted through the same key.

3) Database (DBC) is recommended when operations involve multiple columns; in this instance, it is convenient to use the special encryption key that is generated and implicitly shared among all the columns of the database characterized by the same secure type. The choice of the field confidentiality levels makes it possible to execute SQL statements over encrypted data while allowing a tenant to minimize key sharing.

Metadata Management:

In this module, we develop Meta data. So our system does not require a trusted broker or a trusted proxy because tenant data and metadata stored by the cloud database are always encrypted. In this module, we design such as Tenant data, data structures, and metadata must be encrypted before exiting from the client.The information managed by SecureDBaaS includes plaintext data, encrypted data, metadata, and encrypted metadata. Plaintext data consist of information that a tenant wants to store and process remotely in the cloud DBaaS. SecureDBaaS clients produce also a set of metadata consisting of information required to encrypt and decrypt data as well as other administration information. Even metadata are encrypted and stored in the cloud DBaaS. SecureDBaaS stores metadata in the metadata storage table that is located in the untrusted cloud as the database. This is an original choice that augments flexibility, but opens two novel issues in terms of efficient data retrieval and data confidentiality. To allow SecureDBaaS clients to manipulate metadata through SQL statements, we save database and table metadata in a tabular form. Even metadata confidentiality is guaranteed through encryption. This table uses one row for the database metadata, and one row for each table metadata.

Metadata generated by Secure DBaaS contain all the information that is necessary to manage SQL statements over the encrypted database in a way transparent to the

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

user. Metadata management strategies represent an original idea because Secure DBaaS is the first architecture storing all metadata in the untrusted cloud database together with the encrypted tenant data. Secure DBaaS uses two types of metadata.
1) Database metadata are related to the whole database. There is only one instance of this metadata type for each database.
2) Table metadata are associated with one secure table.

Each table metadata contains all information that is necessary to encrypt and decrypt data of the associated secure table.
1) Column name: the name of the column of the secure table. This is the only information that links a column to the corresponding plaintext column because column names of secure tables are randomly generated.
2) Secure type: This allows a SecureDBaaS client to be informed about the data type and the encryption policies associated with a column. 3) Encryption key: the key used to encrypt and decrypt all the data stored in the column.

Sequential SQL Operations:

The first connection of the client with the cloud DBaaS is for authentication purposes. Secure DBaaS relies on standard authentication and authorization mechanisms pro-vided by the original DBMS server. After the authentication, a user interacts with the cloud database through the Secure DBaaS client. Secure DBaaS analyzes the original operation to identify which tables are involved and to retrieve their metadata from the cloud database. The metadata are decrypted through the master key and their information is used to translate the original plain SQL into a query that operates on the encrypted database. Translated operations contain neither plaintext database (table and column names) nor plaintext tenant data. Nevertheless, they are valid SQL operations that the Secure DBaaS client can issue to the cloud database. Translated operations are then executed by the cloud database over the are received by the Secure DBaaS client, decrypted, and delivered to the user. The complexity of the translation process depends on the type of SQL statement [11].

The SQL operations in Secure DBaaS by considering an initial simple scenario in which we assume that the cloud database is accessed by one client. Our goal here is to highlight the main processing steps, hence we do not take into account performance optimizations and concurrency issues. The first connection of the client with the cloud DBaaS is for authentication purposes.

Secure DBaaS relies on standard authentication and authorization mechanisms provided by the original DBMS server. After the authentication, a user interacts with the cloud database through the Secure DBaaS client. Secure DBaaS analyzes the original operation to identify which tables are involved and to retrieve their metadata from the cloud database. The metadata are decrypted through the master key and their information is used to translate the original plain SQL into a query that operates on the encrypted database. Translated operations contain neither plaintext database (table and column names) nor plaintext tenant data. Nevertheless, they are valid SQL operations that the Secure DBaaS client can issue to the cloud database. Translated operations are then executed by the cloud database over the encrypted tenant data. As there is a one to-one correspondence between plain text tables and encrypted tables, it is possible to prevent a trusted database user from accessing or modifying some tenant data by granting limited privileges on some tables. User privileges can be managed directly by the untrusted and encrypted cloud database. The results of the translated query that includes encrypted tenant data and metadata are received by the Secure DBaaS client, decrypted, and delivered to the user. The complexity of the translation process depends on the type of SQL statement.

Concurrent SQL Operations:

Concurrent execution of SQL statements issued by multiple independent (and possibly geographically distributed) clients is one of the most important benefits of Secure DBaaS with respect to state-of-the-art

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

solutions. Our architecture must guarantee consistency among encrypted tenant data and encrypted metadata because corrupted or out-of-date metadata would prevent clients from decoding encrypted tenant data resulting in permanent data losses. A thorough analysis of the possible issues and solutions related to concurrent SQL operations on encrypted tenant data and metadata available in the online supplemental material.

Here, we remark the importance of distinguishing two classes of statements that are supported by Secure DBaaS: SQL operations not causing modifications to the database structure, such as read, write, and update operations involving alterations of the database structure through creation, removal, and modification of database tables (data definition layer operators). As there is a one-to-one correspondence between plaintext tables and encrypted tables, it is possible to prevent a trusted database user from accessing or modifying some tenant data by granting limited privileges on some tables. User privileges can be managed directly by the untrusted and encrypted cloud database.

The results of the translated query that includes encrypted tenant data and metadata.In scenarios characterized by a static database structure, Secure DBaaS allows clients to issue concurrent SQL commands to the encrypted cloud database without introducing any new consistency issues with respect to unencrypted databases. After metadata retrieval, a plaintext SQL command is translated into one SQL command operating on encrypted tenant data.

As metadata do not change, a client can read them once and cache them for further uses, thus improving performance. Secure DBaaS is the first architecture that allows concurrent and consistent accesses even when there are operations that can modify the database structure. In such cases, we have to guarantee the consistency of data and metadata through isolation levels, such as the snapshot isolation that we can demonstrate work for most usage scenarios.

SYSTEM ARCHITECTURE:

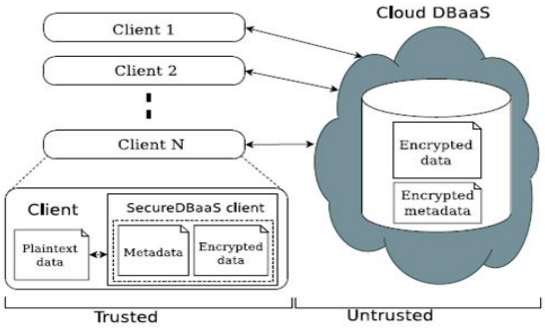


Fig. 1

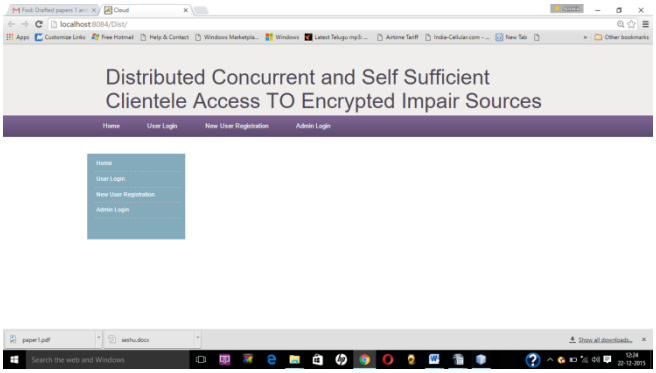
Fig. 1 describes the overall architecture. We assume that a tenant organization acquires a cloud database service from an untrusted DBaaS provider. The tenant then deploys one or more machines (Client 1 through N) and installs a SecureDBaaS client on each of them. This client allows a user to connect to the cloud DBaaS to administer it, to read and write data, and even to create and modify the database tables after creation. SecureDBaaS is designed to allow multiple and independent clients to connect directly to the untrusted cloud DBaaS without any intermediate server.

RSA ALGORITHM

- Select two large prime numbers p, q
- Compute n = p × q v = (p-1) × (q-1)
- Select small odd integer k relatively prime to v gcd(k, v) = 1
- Compute d such that (d × k)%v = (k × d)%v = 1
- Public key is (k, n)
- Private key is (d, n)

SCREENSHOTS

Home page

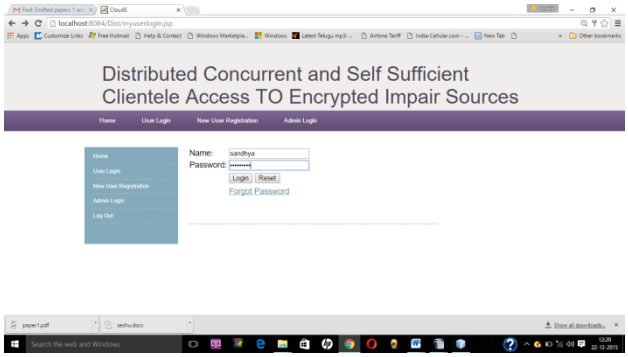


1. Home Page

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

In this page we having the Modules like New user Registration,User Login,Admin Login

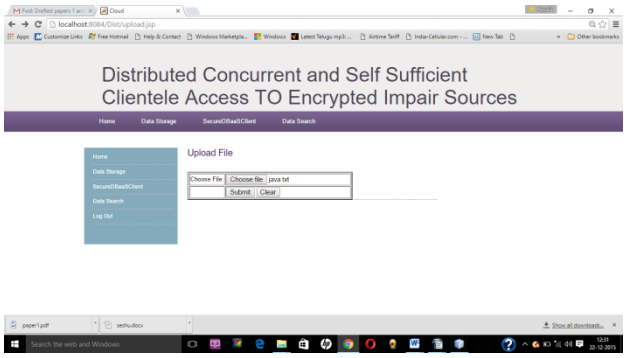
USER LOGIN PAGE



2. Login Page

In this page user enters the valid username and password, if username and password match then user will redirect to user homepage if not match display the error message and stay in the same page.

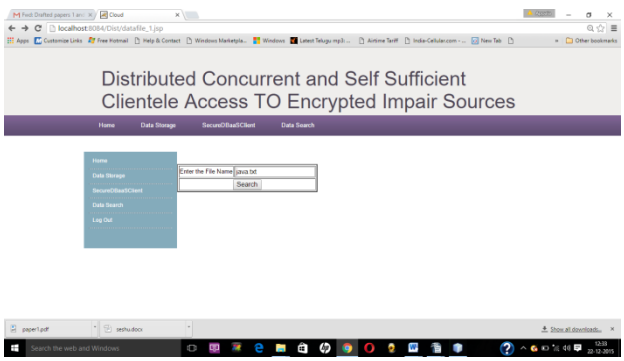
UPLOAD FILE



3. File Upload

In this page user select a file and upload it, at the same time encrypted key is sent to the mail.

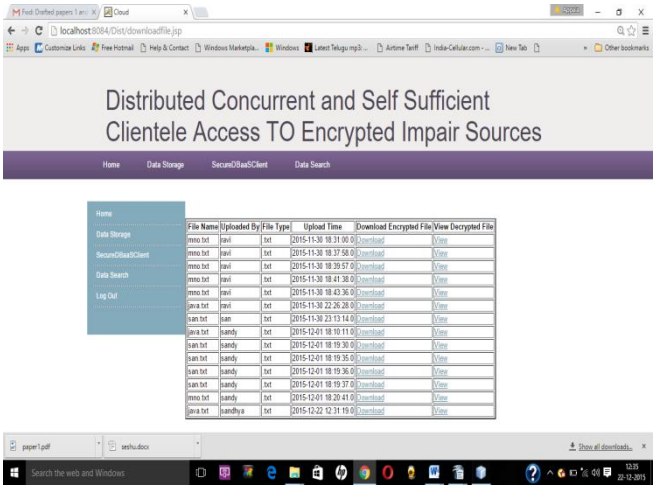
SEARCH THE FILE



4. Search File

In this page user search for a file, if file exists display the file, file not exists display the error message.

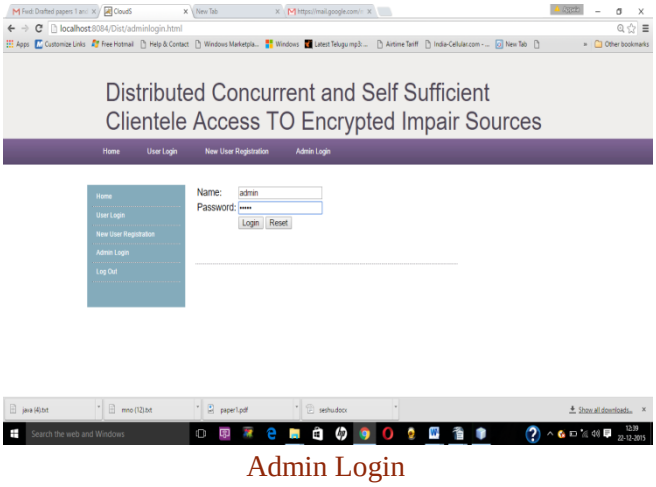
FILES LIST TO VIEW AND DOWNLOAD ENCRYPTED FILE



5. Files List

In this module user can display the file uploaded previously and download the encrypted file and the file contents can be viewed using the valid key.

ADMIN LOGIN

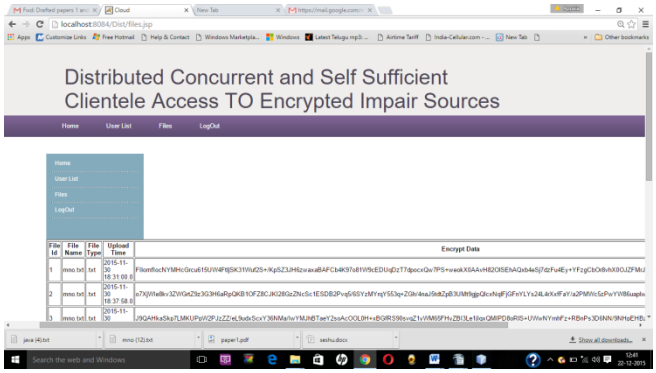


Admin Login

In this page admin enters the admin username and password; if it matches admin will be redirected to admin home page and if username and password not match it display the error message and stay in the same admin login page.

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

ENCRYPTED FILES LIST



Files list

In this page admin can view all the uploaded encrypted files.

CONCLUSION

Concurrent and independent access to encrypted cloud databases, proposes an innovative architecture that guarantees confidentiality of data stored in public cloud databases. The proposed system will not require modifications to the cloud database, and it will be immediately applicable to existing cloudDBaaS. A large part of the research includes solutions to support concurrent SQL operations (including statements modifying the database structure) on encrypted data issued by heterogenous and possibly geographically dispersed clients. 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

FUTURE WORK:

It is worth observing that experimental results based on the TPC-C standard benchmark show that the performance impact of data encryption USING RSA algorithm on response time becomes negligible because it is masked by network latencies that are typical of cloud scenarios and for authentication sending the key to the mail server . In particular, concurrent read and write operations that do not modify the structure of the encrypted database cause negligible overhead. Modifications of the database structure are supported, but at the price of high computational costs. These performance results open the space to future improvements that we are investigating Dynamic scenarios characterized .possibly In the future we will focus on VM's to reduce the cost.

REFERENCES:

[1].Huiqi Xu, Shumin Guo, and Keke Chen,"Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 2, FEBRUARY 2014.

[2].HuiqiXu,ShuminGuo,andKekeChen,"BuildingConfidentialandEfficientQueryServicesintheCloudwithRASPDataPerturbation",IEEETransactionsonknowledgeanddataengineering,VOL.26,NO.2,February2014.

[3].H.Kllapi, D.Bilidas, I.Horrocks, Y.Ioannidis, E.Jiménez-Ruiz, E.Kharlamov, M.Koubarakis, D.Zheleznyakov,"DistributedQueryProcessingontheCloud: the Optique PointofView", InOWLExperiencesandDirections Workshop (OWLED2013). Montpellier, France.May26-30,2013.

[4].P.RavinderRao,S.V.Sridhar,V.Ramakrishna,"An Optimistic Approach for Query Constructionand ExecutioninCloudComputingEnvironment",inIJARCSS, vol.3,Issue5,May2013Issn:2277128X

[5].AtulPhad,SwapnilPatil,SujeetPurane,VineetPatil,"CloudBasedSQLQueryProcessor", in International Journal Of Engineering And Science,Issn:2278-4721,Vol.2,Issue4(February2013),Pp01-04.

[6].K.Chen, R.Kavuluru, and S.Guo, "Rasp:Efficient multi dimensional range query on attack-resilienten crypted databases, "in ACM Conference on DataandApplicationSecurityandPrivacy,2011,pp.249–260.

[7].M. L.Liu, G. Ghinita, C.S.Jensenand P. Kalnis,"Enabling searchservices onoutsourcedprivate patialdata",TheInternationalJournalofonVeryLargeDataBase,vol.19,no.3,2010.

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

[8].Jing Zhao, Xiangmei Huand Xiaofeng Meng,"ESQP: An Efficient SQL Query Processing for Cloud Data Management",inProceedingsofthesecondinternationalworkshoponClouddatamanagement.NewYork,NY,USA:ACM978-1-4503-0380-4/10/10,Pages1-8.

[9].M.Armbrust,A.Fox,R.Griffith,A.D.Joseph,R.K.andAndyKonwinski,G.Lee,D.Patterson,A.Rabkin,I.Stoica,and M.Zaharia,"Abovetheclouds:Aberkeleyviewofcloudcomputing,"TechnicalReport,UniversityofBerkerley,2009.

[10].K.Chen,L.Liu,andG.Sun,"Towardsattack-resilient geometricdataperturbation,"inSIAMDataMiningConference,2007.

[11].R.Agrawal,J.Kiernan,R.Srikant,andY.Xu,"Orderpreservingencryptionfornumericdata,"inProceedingsofACM SIGMODConference,2004.