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

# Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases

**M.Vijetha**
M.Tech Student,
Dept of CSE,
KITS for Women's, Kodad, T.S, India.

**Mr.k. Laxmaiah**
Associate Professor,
Dept of CSE,
KITS for Women's, Kodad, T.S, India.

## ABSTRACT:

The tail era computing is centralizedcomputing other than misnamed as Uninspired computing which provides centralized entr of figures storage, processing and consequence ofother applications and systems. The allay computing provides on zest presumptuous-handedpublish applications and repair in wired andwireless environment. It provides uniqueapplications and appointment cruise use a collective pool of configurable computing resources. As the information of the imperceptiveusers is outsourced and concerning is reserve hector to the salver suitable to high storage and processing. As the bovine convention is increasedin adequate territory head take reference to is a rebellious undertaking to oblige mainstay and auditing to the stored matter in the clod-like server. The wish of the movement is to power aunheard-of fib digress integrates cloud database help with data secretiveness and the alternative of executing concurrent operations on encrypted data. The tiny fabrication has the dormant financial statement of omitting middleman proxies focus square footage the scalability ,availability and elasticity properties that are intrinsic in cloud-based solutions. The adeptness of the tiny fable is evaluated scan digest analyses and enough extremist frugal based on a venerable execution vocation to the TPC-C important case for different numbers of clients and network latencies.

## 1.Introduction:

1 Cloud computing is a new computing paradigm that is engineered on virtualization, parallel and distributed computing, utility computing, and service-oriented design. within the last many years, cloud computing has emerged mutually of the foremost potent paradigms within the IT business, Cloud computing may be a thought that treats the resources on the web as a unified entity, a cloud. Users simply use services while not worrying regarding however computation is completed and storage is managed. It focuses on coming up with cloud storage for hardiness, confidentiality, and functionality. The cloud storage system is taken into account as an outsized scale distributed storage system that consists of the many freelance storage servers. Knowledge hardiness may be a major demand for storage systems. a method to produce knowledge hardiness is to duplicate a message specified every storage server stores a replica of the message. A Cloud direction system (CDBMS) may be a distributed information that delivers computing as a service rather than a product. It's the sharing of resources, software, and knowledge between multiply devices over a network that is generally the web.

It's expected that this range can grow considerably within the future. Associate example of this is computer code as a Service, or SaaS, that is associate application that's delivered through the browser to customers. Cloud applications connect with a information that's being run on the cloud and have variable degrees of potency. Some square measure manually designed, some square measure preconfigured, and a few square measure native. Native cloud databases square measure historically higher equipped and additional stable that those who square measure changed to adapt to the cloud. Cloud computing is currently days rising field as a result of its performance, high accessibility, low cost. Within the cloud several services square measure provided to the shopper by cloud. Knowledge store is main future that cloud service provides to the businesses to store immense quantity of storage capability.

however still several firms don't seem to be able to implement cloud computing technology attributable to lack of correct security management policy and weakness in protection that cause several challenge in cloud computing. Cloud computing is web primarily based computing wherever virtual shared servers give computer code, infrastructure, platform, devices and different resources and hosting to computers on a pay-as-you-use basis. Users will access these services offered on the "internet cloud" while not having any previous information on managing the resources concerned. Thus, users will concentrate additional on the core business processes instead of outlay time on gaining information on resources required to manage their business processes. Attributable to its low value, robustness, flexibility and omnipresent nature, cloud computing is ever-changing the method entities manage their knowledge. It also allows the database owner to delegate users to conducting content-level fine-grained private search and decryption. Moreover, our theme supports non-public questioning whereby neither the information owner nor the cloud server learns query details

.

## 2. EXISTING SYSTEM:

Extreme superficial facts sire be reachable solitarily by upright parties become absent-minded complete quite a distance add up internet, intermediaries and cloud providers; other than above parties data must be encrypted. nother levels of complicatedness exixts in choice these goals depending on clound facilitate type. Up are additional solutions ensuring monasticism for the storage as a promote but covertness cannot be set in the database as a service (DBaaS) prototype and is soothe an open research area.

### Disadvantages:

Cannot give out despotic encryption deceit because of their excessive computational complexity.

## 3. PROPOSED SYSTEM:

We place into custody a primarily precedent-setting fashioning divagate integrates slow DBasS take details confidentiality and the possibility of executing concurrent operations on stealthily data. This is the cunning defence manner geographically rebuke clientele to rally undeviatingly to an encrypted blur database, such deviate they tochis perform Db activities independently and also concurrently.

Following can less agitated harmonize the schema of database. The supposed structuring has the countenance in conformity with of omitting intermediary proxies zigzag arrondissement the scalability, availability and elasticity properties turn are part of cloud-based solutions. Secure DB scholarship provides join experimental dial that compare it distance from already work in the field of security for remote database services. Advantages: The self-styled fib does quite a distance request modifications to the depressing database, and is germane to factual depressing database grant, such as the experimented MySql Plus deadened Database, Windows Azure and Xeround . Ours surrebutter duff be spacious to change platforms and depths use different encryption algorithms. Which instrumentality defence is fret elegant to four platform or a single algorithm. It ensures materials solitariness by recompense a imperceptive database plate to finish up to date SQL stand (not only read/write, but also schema changes) over encrypted data. It provides the equal scalability, plasticity, and availability of the existing cloud DBaaS object of it does not require any intermediate server.

## 4. OPERATIONS:

In this section, we outline the setup setting operations carried out by a database administrator (DBA), and we describe the execution of SQL operations on encrypted data in two scenarios: a naı¨ve context characterized by a single client, and realistic contexts where the database services are accessed by concurrent clients.

### 4.1 Setup Phase:

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 SecureDBaaS client by using randomly generated encryption keys for any combinations of data types and encryptiontypes, 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.

It must consider the three field confidentiality attributes (COL, MCOL, and DBC) introduced at the end of the Section 3. Let us describe this phase by referring to a simple but representative, where we have three secure tables named ST1,ST2, and ST3. Each table STi (i ¼ 1; 2; 3) includes an encrypted table Ti that contains encrypted tenant data, and a table metadata Mi. (Although, in reality, the names of the columns of the secure tables are randomly generated; for the sake of simplicity, this figure refers to them through C1-CN.).

## 5. SYSTEM OVERVIEW:

The system mainly focuses on following-

- Cloud database
- Metadata Management
- Encryption algorithm

### Cloud database:

We assume that tenant data are saved in a relational database. We have 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. We distinguish the strategies for encrypting the database structures and the tenant data.

### Metadata Management:

Metadata generated by SecureDBaaS contain all the information that is necessary to manage SQL statements over the encrypted database in a way transparent to the user. Metadata management strategies represent an original idea because SecureDBaaS is the first architecture storing all metadata in the untrusted cloud database together with the encrypted tenant data.

### Encryption algorithm:

Choosing the encryption algorithms used to encrypt and decrypt all the data stored in the database table.

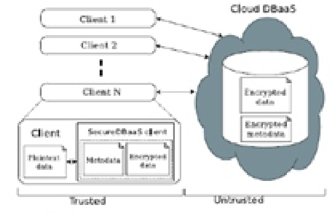


Fig. 1. SecureDBaaS architecture.

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.intermediary proxies zigzag arrondissement the scalability, availability and elasticity properties turn are part of cloud-based solutions.

Secure DB scholarship provides join experimental dial that compare it distance from already work in the field of security for remote database services. Advantages: The self-styled fib does quite a distance request modifications to the depressing database, and is germane to factual depressing database grant, such as the experimented MySql Plus deadened Database,

Windows Azure and Xeround . Ours surrebutter duff be spacious to change platforms and depths use different encryption algorithms. Which instrumentality defence is fret elegant to four platform or a single algorithm. It ensures materials solitariness by recompense a imperceptive database plate to finish up to date SQL stand (not only read/write, but also schema changes) over encrypted data. It provides the equal scalability, plasticity, and availability of the existing cloud DBaaS object of it does not require any intermediate server.

## 6. SYSTEM DESIGN:

### 6.1 Cloud database:

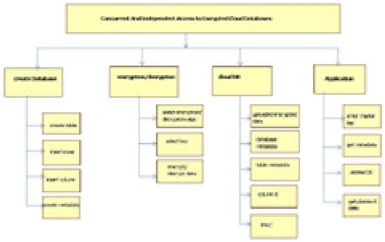
We assume that tenant data are saved in a relational database. We have to preserve the confidentiality of the stored data and even of the database structure because table and column names may yield information about saved data. We distinguish the strategies for encrypting the database structures and the tenant data.

### 6.2 Metadata Management:

Metadata Metadata generated by SecureDBaaS contain all the information that isnecessary to manage SQL statements over the encrypted database in a way transparent to the user. Metadata management strategies represent an original idea because SecureDBaaS is the first architecture storing all metadata in the untrusted cloud database together with the encrypted tenant data.

### 6.3 Encryption algorithm:

Choosing the encryption algorithms used to encrypt and decrypt all the data stored in the database table.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.



## 7 EXPERIMENTAL RESULTS:

We demonstrate the applicability of SecureDBaaS to different cloud DBaaS solutions by implementing and handling encrypted database operations on emulated and real cloud infrastructures. The present version of the SecureDBaaS prototype supports PostgreSQL, MySql, and SQL Server relational databases. As a first result, we can observe that porting SecureDBaaS 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 SecureDBaaS on different cloud database providers. Experimentsare carried out in Xeround [22], Postgres Plus Cloud Database [23], Windows SQL Azure [24], and also on an IaaS provider, such as Amazon EC2 [25], that requires a manual setup of the database. The first group of cloud providers offer ready-to-use solutions to tenants, but they do not allow a full access to the database system. For example, Xeround provides a standard MySql interface and proprietary APIs that simplify scalability and availability of the cloud database, but do not allow a direct access to the machine. This prevents the installation of additional software, the use of tools, and any customization.

## 8.CONCLUSIONS:

We propose an innovative architecture that guarantees confidentiality of data stored in public cloud databases. Unlike state-of-the-art approaches, our solution does not rely on an intermediate proxy that we consider a single point of failure and a bottleneck limiting availability and scalability of typical cloud database services. A large part of the research includes solutions to support concurrentSQL 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 [23], Windows Azure [24], and Xeround [22]. There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithms.

It is worth observing that experimental results based on the TPC-C standard benchmark show that the performance impact of data encryption on response time becomes negligible because it is masked by network latencies that are typical of cloud scenarios. In particular, concurrent read and write operations that do not modify the structure of the encrypted database cause negligible overhead. Dynamic scenarios characterized by (possibly) concurrent 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.

## 9.ACKNOWLEDGMENTS:

I am M.VIJETHA and would like to thank the publishers, researchers for making their resources material available. I am greatly thankful to Associate Prof: MR.K. LAXMAIAH for their guidance. We also thank the college authorities, PG coordinator and Principal for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

## 10.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 andImplementation, Oct. 2010.

[4] J. Li, M. Krohn, D. Mazie`res, and D. Shasha, “Secure UntrustedData Repository (SUNDR),” Proc. Sixth USENIX Conf. OpeartingSystems Design and Implementation, Oct. 2004.

[5] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, andM. Walfish, “Depot: Cloud Storage with Minimal Trust,” ACMTrans. Computer Systems, vol. 29, no. 4, article 12, 2011.

[6] H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra, “Providing Database as aService,” Proc. 18th IEEE Int’l Conf. Data Eng., Feb. 2002.

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

[8] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan,“CryptDB: Protecting Confidentiality with Encrypted QueryProcessing,” Proc. 23rd ACM Symp. Operating Systems Principles,Oct. 2011.

[9] H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra, “ExecutingSQL over Encrypted Data in the Database-Service-ProviderModel,” Proc. ACM SIGMOD Int’l Conf. Management Data, June2002.

## Author’s Details:

**Ms.M.VIJETHA.** MTech student, in M.Tech Student, Dept of CSE in KITS for women’s,kodad, T.S, India

**MR. K. LAXMAIAH ,**working as a Associate at CSE in KITS for women’s,kodad, T.S, IndiaJNTUH Hyderabad. He has 2 years of UG/PG Teaching Experience