## Abstract

Nowadays cloud computing and data security are becoming very popular issues in data storage. In case of handover any critical data in the hands of a cloud service provider should serve with the guarantee of security and availability for data at any time anywhere, but for every data transmission or handover situation we need to secure our data, so we need data encrypted must be every time before it should handover, now we are providing a solution supporting off premises distributed clients to connect directly to an encrypted cloud database, and to update or use that data by independent operations. In our proposed system has the advantage of neglecting intermediate proxies that limit the availability, scalability, security and elasticity, properties that are beneficial in cloud-based solutions. In this paper we are going to study different research papers based on our topic. Also we state the difference between different cloud database security systems. Also in this system we are working to understand Cloud DBaaS architecture.

### 1. Introduction

Personal computers are storing all types of data like text documents, images, sound recordings, videos, programs, software’s, scientific information, and so on. As on this data we are going to apply update, visualization, compilation, these tasks are called as data management. Data
management systems generally store large quantities of information representing the historical records of an organization. It's vital that the recent data and applications still work as new data and applications are value added. The systems are in constant amendment. Indeed, most of the larger information systems operational nowadays were designed many decades past and have evolved with technology. A historical perspective helps to know current systems. There are six distinct phases in data management. Initially, data was manually processed. Next evolution was punched card instrumentation and electro-mechanical machines which is used to type and tabulate lots of records. The next phase was used to hold data on magnetic tape and to perform execution on serial files. The fourth generation introduced the conception of a database schema and on-line navigational relational databases and value-added distributed and client server process. The early stages of sixth generation systems that have more data types, notably documents, images, voice, and videos. These sixth generation systems are the storage engines for the rising internet and Intranets.

2. System Architecture

![Basic System Architecture](image)

**Figure 1: Basic System Architecture**

**2.1 Survey Of Different Architecture**

**a) Distributed, concurrent, and independent access to encrypted cloud databases**

*(By Luca Ferretti, Michele Colajanni, and Mirco Marchetti)*

In this article 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. The efficacy of the proposed 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.
b) Survey on the Concurrency Control Protocols for Encrypted Cloud Databases
   (By-Dr. M. Newlin Rajkumar, Brighty Batley C, Dr.V.Venkatesakumar, Ancy George)
Cloud database environments are very attractive for the deployment of large scale applications due to their highly scalable and available infrastructure. The main reason for the users deploying different types of applications in the cloud is its pay-for-use cost model. This survey contains the most prominent concurrency control protocols that can be used in the encrypted cloud database. The degree of data consistency and cost requirements varies according to the concurrency control protocols.

c) Privacy Preserving Approach using Encrypted Cloud Databases (By-Shital H. Dinde, Arati M. Dixit)
Rapid advances in storage, communications, and processing allow us to move all data into cyberspace. Data management systems began by automating traditional tasks like keeping record of business transactions. This data consisted primarily of numbers and character strings. Today the automated systems offer the infrastructure for our society, allowing quick, reliable, secure, and automatic access to information distributed throughout the world. One of that service provider system is cloud. Currently the enterprises are moving towards less cost, more availability, agility, managed risk, all of that is accelerated towards Cloud Computing. Cloud is not a specific product, but a simplest way of delivering IT services that are serviced on demand, elastic to rescale as needed, and follow a pay-for-usage model. Out of the three common kinds of cloud computing service models, Infrastructure as a Service (IaaS) is a service model that provides servers, computing power, network bandwidth and Storage capacity, as a service to their subscribers. Cloud will relate to many things but without the basic storage items that is provided as a service particularly Cloud Storage, none of the other applications is feasible. But there are many security issues in cloud storage. The solution for that is to work on encrypted data i.e. store the data into the cloud database in encrypted format and operate on that encrypted data and directly connect distributed client to encrypted cloud database i.e. without intermediate proxies.

d) Independent Access to Encrypted Cloud Databases (By-M.Stalin, S.Hemaswathi )
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.

e) Building Encrypted Data Over Mas By Achieving Data Confidentiality (By-V.Muthurani, A.Lourdesmary)
In a cloud arena, inserting important information below untrusted third parties, risks the confidentiality of data. Guaranteeing confidentiality within the Database as a service (DBaaS) paradigm remains a problem. Therefore to resolve that Confidential Concurrent to Secure DBaaS is projected because the initial resolution to produce availability, security, accessibility and reliability while not exposing unencrypted information to the cloud provider. It additionally permits multiple,
freelance and regionally distributed clients to execute synchronic operations on encrypted and preserve information confidentiality and consistency at the consumer and cloud level. It eliminates any intermediate server between the cloud consumer and also the cloud provider. To realize this, Confidential concurrent to Secure DBaaS integrates existing cryptographic schemes, isolation mechanisms and management of encrypted information on the untrusted cloud information.

3. Advantages of Proposed System
In this proposed architecture may not require some modifications in to the cloud database, and it is directly applied on existing cloud DBaaS.

i.) It provides the availability and scalability of the original cloud DBaaS because it does not require any data transaction intermediate server.

ii.) There are no any practical limits to extend our solution to other platforms and to include new encryption algorithm.

iii.) 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.

4. Conclusion
In this paper we studied Secure Distributed Encrypted Cloud Databases planned to that enable cloud to require full advantage of DBaaS total security aspects to our rolling data among cloud. Also in this paper we studied different cloud base security papers from different journals and different research websites. The different concurrency controls in the encrypted cloud database such as SO-ISR, SI, SC and C3 is discussed. Secure DBaaS uses the isolation mechanisms for providing concurrent access to its geographically distributed clients.

5. References


