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

A Framework that integrates cloud database services with confidentiality, at the same time as removing intermediate proxies.

C H R Upender Chary
MTech Student
Department of CSE
St.Peter's Engineering College,
Hyderabad, TS, INDIA

Dr.N.Chandra Sekhar Reddy
Professor & HoD
Department of CSE
St.Peter's Engineering College,
Hyderabad, TS, INDIA

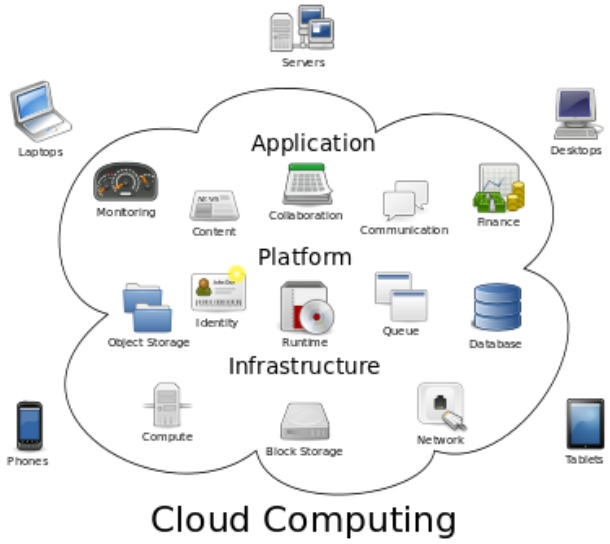
T Shilpa
Assistant Professor
Department of CSE
St.Peter's Engineering College,
Hyderabad, TS, INDIA

Abstract:
Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is one of the renowned and fascinating technology all over the world. It consists of various hardware and software resources made available on internet. Many times large number of sensitive data available on cloud. With the growth of the cloud users malicious activity in the cloud has been increased day by day. Millions of people are using services over cloud database, so it becomes more secured and integrity of data should be maintained. The proposed system consists of creation of multiple virtual clouds. Security of data over cloud would be maintained by using various encryption algorithms. Concurrent and secured sharing of data on cloud database would be maintained.

Keywords: ***Cloud, Encryption, Decryption, Virtual clouds, Databases***

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

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 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, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual

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

resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated 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 monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

From the security viewpoint, various risks and issues are discussed for data over cloud. There are various threats associated with the security but one of the major issues is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. Although Cloud computing has achieved a great success in various industries whether it is a software industry, a Government Organization or a Healthcare sector, but this transition to Cloud computing has various concerns on a critical issue for the success of information systems, communication and information security. There are various risks associated with the security but one of the major issues is the security of data being stored on the provider's cloud database and privacy while the data is being transmitted. So to make Cloud computing technology more secure; for concurrent access to data on cloud database and for independent access of data on cloud database; a framework is proposed to encrypt the data over cloud database using various encryption algorithms.

Related Work:

Luca Ferretti, Michele Colajanni, and Mirco Marchetti proposed a novel architecture for describing possibility of executing concurrent operations on encrypted data and integrates cloud database services with data confidentiality [1].Sushmita Raj, Milos Stojmenovi and Amiya Nayak proposed a new decentralized access control scheme .In that cloud verifies the authenticity of unknown user before storing data [2]. Julisch K. & Hall. M. proposed importance of Virtualization, Web Service, Service Oriented Architecture and Application Programming Interfaces for cloud computing [13].

Gellman discussed standards for collection, maintenance and disclosure of personal information over cloud[20]. Jarabek and Hyde described possible attacks on cloud data [12][15].Guo Yubinet al, had done work on storage solution for No SQL database using homomorphic encryption algorithms. Data querying Protocol described in this work and algorithms for data manipulation are given also[5].Ming Li et al, proposed a novel framework of secure sharing of personal health records over clouds. Considering partially trustworthy cloud servers, patients will be able to maintain their own privacy through encrypting their PHR files to allow fine-grained access [6].Omer K. Jasim et al, discussed the various encryption symmetric key algorithms and asymmetric key algorithms. They also discussed the performance of encryption algorithms on a cloud environment for input blocks of different sizes and how the change in the size of the files after encryption is complete [7].T. Sivasakthi and Dr. N. Prabakaran proposed use of digital signature for authentication purpose in cloud computing. The propose work assured to secure the information in cloud server[3].Sanjoli Singla, Jasmeet Singh proposed a design that can help to encrypt and decrypt the file at the user side that provide security to data at rest as well as while moving. For this Rijndael encryption algorithm along with EAP-CHAP used [4].

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

Kuyoro S. O.described key security considerations and challenges which are currently faced in the Cloud computing [8]. J. Bethencourt et al, discussed Attribute Based Scheme (ABE). For this, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs that are In key-policy and Cipher text-policy [17]. ENISA(European Network Information and Security Agency)investigated the different security risks related to adopting cloud computing along with the affected areas, various risks, impacts, and vulnerabilities in the cloud computing may lead to such risks[18]. Balachandra et al, discussed the security SLA‟s specification and objectives related to data locations, segregation and data recovery[16].Kresimir et al, discussed high level security concerns in the cloud computing model[14]. Bernd et al, discussed the how security weaknesses existing in the cloud platform and how they affect the client data. [20]. Cloud Security Alliance (CSA) had given TOP threats to cloud computing [19].Service Level Agreements (SLA) also defined many times for data on the cloud [20].

Following are the security issues to be fulfilled while working with cloud database:

a) Privacy and Confidentiality

Once data get dispatched on the cloud database, there will be limited access to that data. Privacy of sensitive data should always be maintained. Appropriate privacy policies and procedures should be there to assure the cloud users of the data safety.

b) Data integrity

Integrity of data should be maintained with security. Cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point.

c) Data location and Relocation

High degree of mobility can be offered by Cloud computing. There should be a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.

d) Data Availability

When data is available on different locations or clouds, integrity of data on cloud database would be maintain. Uninterruptable data should be provided.

Existing System:

In a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality is of paramount importance. This requirement imposes clear data management choices: original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries, 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 a service (DBaaS) paradigm is still an open research area.

Disadvantages of Existing System:

- It is not secure.
- Satisfying these goals has different levels of complexity depending on the type of cloud service.

Proposed System:

The architecture design was motivated by a threefold goal: to allow multiple, independent, and geographically distributed clients to execute concurrent operations on encrypted data, including SQL statements that modify the database structure; to preserve data confidentiality and consistency at the client and cloud level; to eliminate any intermediate server between the cloud client and the cloud provider. The possibility of combining availability, elasticity, and scalability of a typical cloud DBaaS with data confidentiality are demonstrated through a prototype of SecureDBaaS that supports the execution of concurrent and independent operations to the remote encrypted database from many geographically distributed clients as in any unencrypted DBaaS setup. To achieve these goals, SecureDBaaS integrates

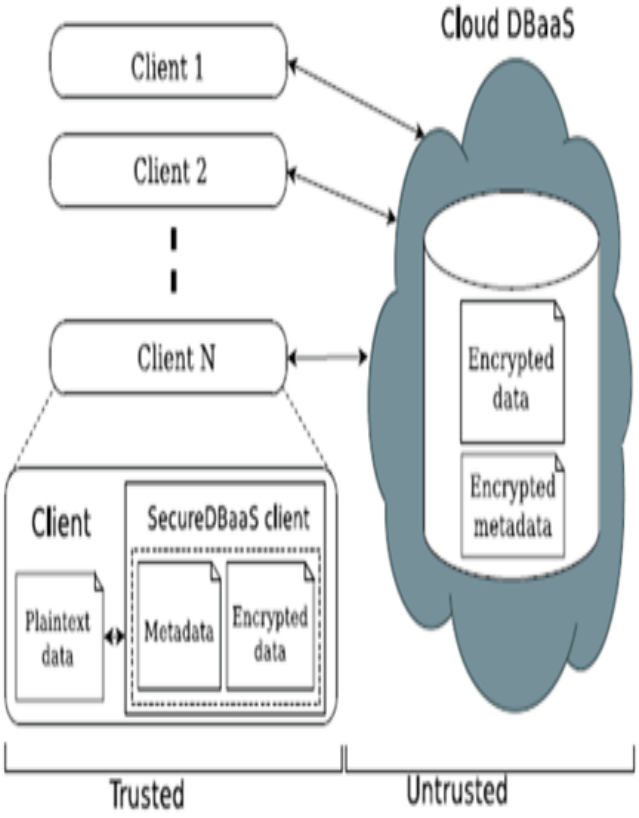
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

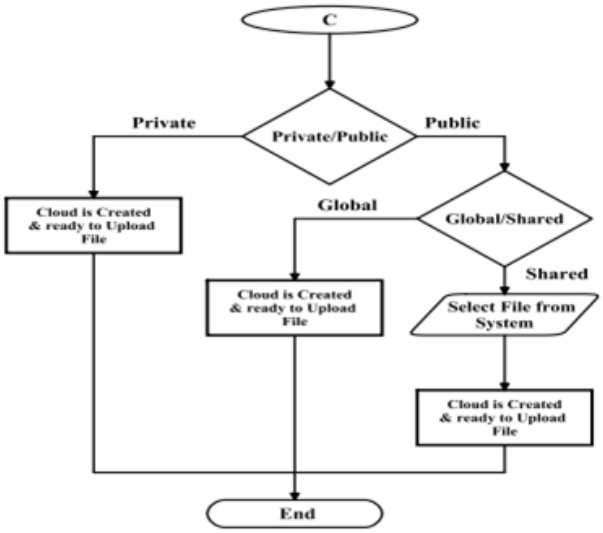
existing cryptographic schemes, isolation mechanisms, and novel strategies for management of encrypted metadata on the untrusted cloud database. This paper contains a theoretical discussion about solutions for data consistency issues due to concurrent and independent client accesses to encrypted data. In this context, we cannot apply fully homomorphic encryption schemes because of their excessive computational complexity.

Advantages of Proposed System:

- The motivation of these results is that network latencies, which are typical of cloud scenarios, tend to mask the performance costs of data encryption on response time.
- SecureDBaaS is immediately applicable to any DBMS because it requires no modification to the cloud database services.

System Architecture:





New Cloud Creation

System Implementation

User Registration:

Many numbers of users will be able to do registration and create their virtual Private clouds by default when registrations get completed.

Input: Information of user will be taken for generation of User-id and Password.

Output: User gets registered and Virtual Private cloud will be created for registered user.

Virtual Cloud Creation:

After registration, users have to Log-in and options will be provided for creation of shared (Public) or Private cloud.

Input: User-id, password, select option for Shared or Private cloud.

Output: Shared or Public cloud created for specific user.

Upload Data over cloud:

Input: Select cloud name for keeping user‟s data file.

Output: User‟s data will be kept on particular cloud for future purpose.

Download Data from cloud:

Input: Select cloud name from which client has to get data which is present over cloud.

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

Output: Client will be provided with required data from selected cloud.

Encryption of Plain Data File:

Input: Generated key and Plain Data File from System.

Output: Encrypted file in Human Unreadable format.

Decryption of Encrypted Data File:

Input: Same key used for Encryption and Encrypted Data File.

Output: Decrypted Data File in Human Readable format.

Conclusion:

Cloud computing offers real various alternatives to IT departments for improved flexibility and lower cost. Many services are readily accessible on a pay-per-use basis and offer great alternatives to businesses that need the flexibility to rent infrastructure on a temporary basis or to reduce capital costs. Proposed a framework which encrypts data before it is uploaded on to the cloud and it also create secured, concurrent and independent encrypted data over cloud. Use of AES algorithm provides secure transfer of Data File within few seconds. Thus, if used securely, cloud computing provides a user with amazing benefits and overcomes its only disadvantage of security thread.

References

1. Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud databases", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 25, no. 2, pp.437-445, FEBRUARY 2014.

2. Sushmita Raj, Milos Stojmenovic, Amiya Nayak," Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 25,no. 2, pp.332-345,February 2014.

3. T. Sivasakthi and Dr. N. Prabakaran, "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing" , International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 2,pp.12-18, February 2014.

4. Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering & Technology ,vol. 2, no. 7,pp.2232-2235, July 2013

5. Guo Yubina, Zhang Liankuanb, Lin Fengrena, Li Ximinga,"A Solution for Privacy-Preserving Data Manipulation and Query on NoSQLDatabase", JOURNAL OF COMPUTERS, VOL. 8, NO. 6, 1427-1432, JUNE 2013.

6. Ming Li, Member, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 24, no. 1, 131-143, JANUARY 2013.

7. Omer K. Jasim, Safia Abbas, Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Efficiency of Modern Encryption Algorithms in Cloud Computing", International Journal of Emerging Trends & Technology in Computer Science,vol.2,no.6,pp.270-274,December 2013.

8. Kuyoro S. O., Ibikunle F., AwodeleO. ,"Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Vol. 3, no.5, 247-255, 2011.

9. Gartner," From Secure Virtualization to Secure Private Clouds", http://www.vmware.com/files/pdf/analysts/Gartner

10. "Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud", https://www.cloudsecurityalliance.org,December,2009.

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

11. Jericho Forum," Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration", April, 2009.

12. C. Jarabek,"A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks, and Management", Department of Computer Science, University of Calgary, 2010.

13. Julisch, K., & Hall, M., "Security and control in the cloud", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309,2010.

14. P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Humanoriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349,2010.

15. D.Hyde,"A Survey on the Security of Virtual Machines", http://www1.cse.wustl.edu/~jain/cse571-09/ftp/vmsec.pdf, April 2009.

16. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC „09 IEEE International Conference on Services Computing, pp. 517-520, 2009.

17. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

18. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing- risk-assessment

19. https://cloudsecurityalliance.org/topthreats/csathreats.v1. 0.pdf.

20. http://en.wikipedia.org/wiki/Cloud_computing.