IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

Independent Access to Encrypted Cloud Databases

M.STALIN
M.E Computer Science and Engineering
Mount Zion College of Engineering and Technology
Pudukkottai,Tamilnadu.
mcstalin27@gmail.com

S.HEMASWATHI
Dept. of Computer Science and Engineering
Mount Zion College of Engineering and Technology
Pudukkottai,Tamilnadu.
hemarajkumar1989@gmail.com

***Abstract*-- 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.**

***Keywords*— Cloud Storage, Security, Independent Access, DBaaS.**

I. PREAMBLE

In this paper we presented the technique to improve the performance through theoretical analysis and experimental evaluation data consistency issues due to concurrent and independent client accesses to encrypted data. In existing system the Can not apply fully homomorphic encryption schemes because of their excessive computational complexity. The User does not have the full control over the database. The database as a Service is a sticky services. No separate security to database. Data loss may occur.

Overall processes in communication between the Owner, User, Cloud .Cloud storage is offered by Storage as a Service , SaaS is a business model in which a large company rents space in their storage infrastructure to a smaller company or individual. Cloud providers manage the infrastructure and platforms that run the applications. saas is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis.

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.

This paper is prepared by the following: The related works are discussed in the 2nd section. The proposed work about the different discussed in the 3rd section. The Results and discussion is discussed in the 4th section. The conclusion and the further research are discussed in the 5th section.

II. RELATED WORK REVIEW

In previous research papers, they are tried to improve the independent Access method in outsourced storage in cloud. They are focusing to improve the reliability of communication .we doesn't focus any illegal interaction compensation. This trusted cloudme give the possible ways to improve the communication, and secured data.

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. Cloud direction system (CDBMS) may be 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

IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

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 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 has been visualized because the next-generation design of IT Enterprise. In cloud computing application computer code and knowledge bases square measure moving to the centralized massive data centers. This mechanism brings regarding several new challenges, that haven't been well understood. Security and privacy considerations, however, square measure among the highest considerations standing within the method of wider adoption of cloud. In cloud computing the most concern is to produce the safety to finish user to safeguard files or knowledge from unauthorized user. Security is that the main intention of any technology through that unauthorized trespasser cannot access your file or knowledge in cloud. we've got styled one planned design and design which will facilitate to write and rewrite the file at the user facet that give security to knowledge at rest yet as whereas moving.

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. However, various privacy concerns arise whenever potentially sensitive data is outsourced to the cloud. The planned theme prevents the cloud server from learning any probably sensitive plaintext within the outsourced databases. 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.

Efficiency and Security: PDP scheme , perform symmetric key operations in setup and verification phases.

Dynamic Data Support: To supports secure and efficient dynamic operations on outsourced data blocks,that are uptation modification, deletion and append.

TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

III. PROPOSED SYSTEM DESIGN

This architecture illustrates in figure 1 the proposed system contain Owner, User, Cloud. Whenever owner store the information in encrypted format using keys.TPA is a controller of owner, user and Cloud. The users are using this system by receiving the message and getting information from Cloud. Cloud Data Base is independent Access between owner and user.

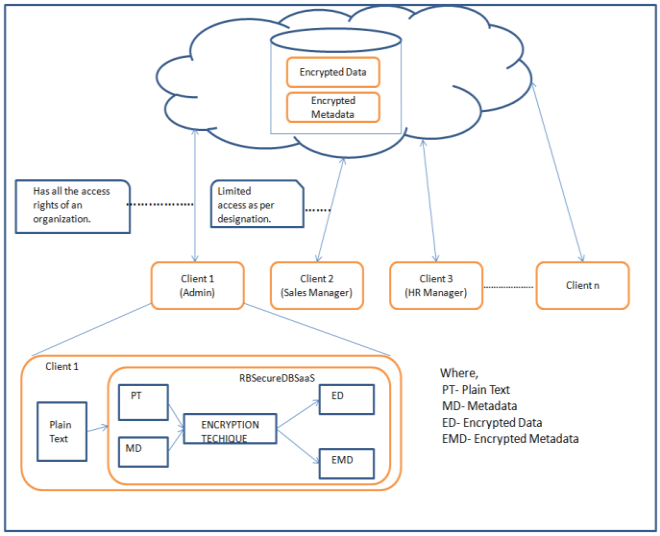


Fig .1. Architecture Diagram

For System Process

User Side

IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

Fig .2. User Side Process

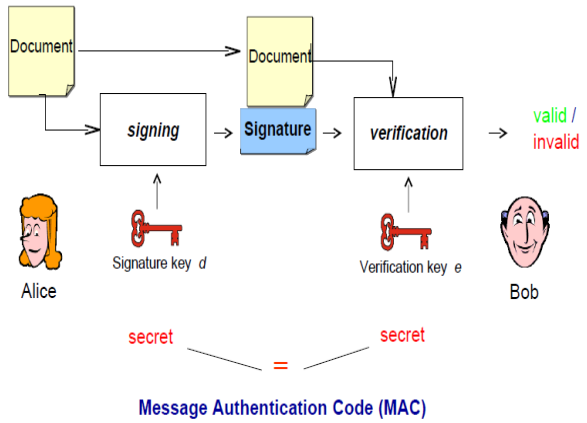
CSP Side

2.	Cloud ask User for authentication just like login page.
4.	Verify password if correct send a file that he wants to access. Else move to step 2.
7.	Cloud check the signature for authenticity and compute the message digest to find encrypted file which is compare with encrypted file of another message.
8.	If correct it will change previous file with this one and move to step12.
9.	Else ask the client to follow the step 8.
10.	CSP sends a same message to client after addition of his signature.

Fig .3. CSP Side Process

A. Message Authentication Code (MAC)

Authenticity, integrity
Electronic Signature (= asymmetric signature)
Authenticity, integrity, non-repudiation
Encryption:
Confidentiality
Encryption: c ≡ me mod n (m is the plaintext)
Decryption: m ≡ cd mod n (c is the cipher text)



Recently Novell announced support for the CloudMe service in their Dynamic File Services Suite. Novosoft Handy Backup version 7.3 also announced support for CloudMe. There are many third party mobile apps and software available for CloudMe, many using the WebDAV support of CloudMe.

1.	User request to access a file from Cloud.
3.	User authenticates CSP by his password
5.	User decrypts the file by applying decryption algorithm
6.	If User modify the file he will send file to CSP and TTP with a message like *Md* as (*F*',$,*M*) and *F* ' here M denotes for modification F ' for encrypted file, *Md* for message digest file and $ for signature.
11.	If file is same as previous one, drop this packet and move to step 1 or step 13.
12.	Else ask CSP to follow step 11 again.
13.	Exit ' F

The users can enhance the use of CloudMe by having iPhone or Android phone. Once CLoudMe is installed on the device, one can easily access the data all over the network. If the user makes changes in the cloud, then all the required changes will be made to other data as well. For instance, if a photo is taken with CloudMe iPhone application and saved in the CloudMe folder, then it will also be available on the computer drive as well. CloudMe can also be installed on multiple computers at the same time, for example, on home and work computer so that you can have all the files available on both the computers. There is no longer a need to have a USB-memory stick with you. Further, CloudMe allows the user synchronize multiple folders simultaneously. Now you can keep your photos, music, videos and documents all organized in the same folder as you always wanted to have but now with an additional CloudMe features.

B. RSA Problem

An Given a cipher text c and a public key (n,e), compute m such that c ≡ me mod n .Mathematical formulation: Compute an e-th root mod n .Factorisation problem (in the context of RSA) Given a natural number n composed of two primes p and q, compute p and q. Attacker is able to decrypt (or sign), if he knows d ,Computation of d is today done via (p-1) · (q-1) , Attacker factors n, i.e. he computes p and q

We propose a significant security improvement to the using novel architecture that integrates cloud database services with data confidentially and the possibility of executing the concurrent operation 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 operation including those modifying the database structure. Secure DbaaS provides several original features that differentiate it

from previous work in the field of security for remote database services.

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 solutions 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.

IV. Result And Discussion

This paper explains Register and upload the files. The upload files using keys, To maintain the privacy of outsourced data in a secure manner. Independent Access between Cloud and data owner. The owner is capable of not only archiving and accessing the data stored by the csp, but also updating and scaling this data on the remote servers.The above discussion explains how to manage seurind data transmission in cloud computing.

V. Conclusion And Future Work

In this paper we have shown overheads on storage, communication and the computation of our data. This will improve the performance of communication and storage security. An innovative architecture that guarantees confidentiality of data stored in public cloud databases. A large part of the research includes solutions to support concurrent SQL operations including statements modifying the database structure on encrypted data issued by heterogeneous and possibly geographically dispersed clients. There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithm. 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. For future work to develop the performance results open the space to future improvements that we are investigating and we will try to resist adversaries with broader background knowledge, such as richer relationship among topics (e.g., exclusiveness, sequentiality, and so on) or capability to capture a series of queries (relaxing the second constraint of the adversary) from the victim. We will also seek more sophisticated method to build the user profile, and better metrics to predict the performance (especially the utility) of UPS.

References

[1]. Amazon elastic compute cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[2]. Hacigumus, B. Iyer, and S. Mehrotra, “Providing Database as aService” Proc. 18th IEEE Int’l Conf. Data Eng., Feb. 2002.

[3]. J. Li, M. Krohn, D. Mazie`res, and D. Shasha, “Secure Untrusted Data Repository (SUNDR)” Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation, Oct. 2004.

[4]. J. Li and E. Omiecinski, “Efficiency and Security Trade-Off in Supporting Range Queries on Encrypted Databases” Proc. 19th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security,Aug. 2005.

[5]. E. Mykletun and G. Tsudik, “Aggregation Queries in the Database-as-a-Service Model” Proc. 20th Ann. IFIP WG 11.3Working Conf. Data and Applications Security, July/Aug. 2006.

[6]. 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 and Implementation, Oct. 2010.

[7]. M. Armbrust et al., “A View of Cloud Computing” Comm. of theACM, vol. 53, No.4, pp. 50-58, 2010.

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

[10]. W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing” Technical Report Special Publication800-144, NIST, 2011.

[11]. Postgres Plus Cloud Database, EnterpriseDB, http://enterprisedb.com/cloud-database , Apr. 2013.

[12]. Xeround: The Cloud Database, Xeround, http://xeround.com Apr. 2013.

[13]. “Windows Azure,” Microsoft corporation, http://www.windowsazure.com , Apr. 2013.

M. Stalin is a M.E., Candidate in the Department of Computer Science and Engineering at Mount Zion College of Engineering and Technology, Pudukkottai. He received his B.E. degree in computer science from Trichy Engineering College, Trichy in 2010. He has undergone his project regarding "Independent Access to Encrypted DataBases".

Asst.Prof S**.Hemaswathi** received her M.E in computer science (2012) from Raja College of Engineering and technology, Madurai & B.E in Computer Science (2010) from Odaiyappa College of Engineering and Technology, Theni, Tamilnadu, India. She is having 2 Years of Experience in Teaching & Currently working as Assistant Professor in the Department of Computer Science and Engineering in MZCET, Pudukkottai. She had published 3 papers in various National Conferences and she had published "Prioritizing application placement for cluster based web application" in Journal of Computer Application.