International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 01
January 2017

An Exploration of Concurrent, and Independent Access to Encrypted Cloud Databases

Chittimalla Sowmyasri
M. Tech, Computer Science &Engineering
Vaagdevi college Of Engineering, Bollikunta, Warangal Dist Telangana State, India.
Mr. Manyam Sukesh
Assistant Professor, Department of CSE
Vaagdevi college Of Engineering, Bollikunta, Warangal Dist Telangana State, India.

Abstract: Putting important data in the hands of a cloud provider must come with the assurance of protection and availability for data at relaxation, in motion, and in use. A few alternatives exist for storage offerings, even as data confidentiality solutions for the database as a provider paradigm are nonetheless immature. Cloud computing can deal with this trouble by offering data storage mechanism to access the data at any place. That is one of the storage gadget used to access their data at wherever via networks which is known as cloud provider. For this service user fear in regards to the safety and privacy challenge beneath this cloud computing for his or her personal data. For this drawback this survey shows quite a lot of tactics for the safety and privacy mechanism for the user data. There are various data storage systems available, but we're seeking to combine cloud database service along with data security and likewise can participate in unbiased and concurrent operations on encrypted data.

Keywords- Cloud Storage, Security, Independent Access, DBaaS.

I. INTRODUCTION

In a cloud context, where critical data is positioned on infrastructures of untrusted third parties making certain data confidentiality is of paramount value. This requirement imposes clear data management picks: original un deniable data must be accessible handiest with the aid of trust data that doesn't include cloud vendors, intermediaries, and web; in any untrusted context, data have got to be encrypted. Gratifying these ambitions has specific stages of complexity depending on the style of cloud carrier. There are a few options making sure confidentiality for the storage as a service paradigm at the same time guaranteeing confidentiality within the data base as a provider(DBaaS) paradigm is still an open study subject. This context proposes comfortable DBaaS as the unconventional resolution that permits cloud tenants to take full advantage of DBaaS traits, such as availability, reliability, and elastic scalability, without exposing unencrypted data to the cloud provider. The architecture design was stimulated by a threefold goal: to allow multiple, independent, and geographically dispersed clients to execute concurrent operations on encrypted data, including SQL statements that regulate the database structure; to keep data confidentiality and consistency at the purchaser and cloud stage; to get rid of any intermediate server between the cloud client and the cloud provider. The possibility of mixing availability, elasticity, and scalability of a usual cloud DBaaS with data confidentiality is established by means of a prototype of secure DBaaS that supports the execution of concurrent and independent operations to the remote encrypted database from many geographically allotted users as in any unencrypted DBaaS setup. To obtain these goals, comfortable DBaaS integrates current cryptographic schemes, isolation mechanisms, and novel techniques for management of encrypted metadata on the untrusted cloud database. This paper contains a theoretical dialogue about options for data consistency issues because of concurrent and unbiased client accesses to encrypted data. In this context, it does not apply thoroughly homomorphism encryption schemes considering the fact that of their excessive computational complexity. The Secure DBaaS

architecture is tailored to cloud platforms and does now not introduce any middle man proxy or dealer server between the client and the cloud provider Workloads together with changes to the database structure are additionally supported through comfortable DBaaS, however at the fee of overheads that appear suitable to obtain the preferred stage of information confidentiality. The motivation of these results is that community latencies, which are normal of cloud situations, are likely to mask the efficiency bills of data encryption on response time.

II. RELATED WORKS

" A View of Cloud Computing" M. Armbrust [1], has developed with innovative ideas for new Internet services no longer require the large capital out lays in hardware to deploy their service or the human expense to operate it. Cloud Computing will grow, so developers should take it in to account. Moreover:

1. Applications Software needs to both scale down rapidly as well as scale up, which is a new requirement. Such software also needs a pay-for-use licensing model to match needs of Cloud Computing.

2. Infrastructure Software needs to be aware that it is no longer running on bare metal but on VMs. Moreover, billing needs to build in from the start.

3. Hardware Systems should be designed at the scale of a container (at least a dozen racks), which will be is the minimum purchase size.

"SPORC: Group Collaboration Using Untrusted Cloud of index. Resources" A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felton [2], have described Cloud-based services are an attractive deployment model for user-facing applications like word processing and calendaring. In SPORC, a server observes only encrypted data and cannot deviate from correct execution without being detected. SPORC allows concurrent, low-latency editing of shared state, permits disconnected operation, and supports dynamic access control even in the presence of concurrency Acknowledgments.

"Secure Untrusted Data Repository(SUNDR)" J. Li, M. Krohn, D. Mazie` res, and D.

Shasha, [3] have proposed SUNDR is a network file system designed to store data securely on untrusted servers. SUNDR's protocol achieves a property called fork consistency, which guarantees that clients can detect any integrity or consistency failures as long as they see each other's file modifications. Measurements of our implementation show performance that is usually close to and sometimes better than the popular NFS file system.

"Depot: Cloud Storage with Minimal Trust" P. Mahajan,S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M.Walfish [4] have described the design, implementation, and evaluation of Depot, a cloud storage system that minimizes trust assumptions. Depot began with an attempt to explore a radical point in the design space for cloud storage: trust no one.

"Providing Database as a Service" H. Hacigu¨ mu¨ s,B. Iyer, and S. Mehrotra [5], have proposed a new paradigm for data management in which a third party service provider hosts "database as a service" providing its customers seamless mechanisms to create, store, and access their databases at the host site. The authors introduced NetDB2, an internet-based database service built on top ofDB2 that provides users with tools for application development, creating and loading tables, and performing queries and transactions.

"Fully Homomorphism Encryption Using Ideal Lattices" C. Gentry [6], has proposed a fully homomorphism encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. The circuit privacy of E2 immediately implies the (leveled) circuit privacy of our (leveled) fully homomorphism encryption scheme.

"Crypt: Protecting Confidentiality with Encrypted Query Processing" R.A.Popa, C.M.S. Redfield, N. Zeldovich, and H.Balakrishnan [7], have described, Crypt is a system that provides practical and provable confidentiality in the face of these attacks for

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 01
January 2017

applications backed by SQL databases. It works by executing SQL queries over encrypted data using a collection of efficient SQL-aware encryption schemes.

"Efficiency and Security Trade-Off in Supporting Range Queries on Encrypted Databases" J. Li and E.Omiecinski [8], had discussed concerns about protecting sensitive information of data and queries from adversaries in the DAS model. Data and queries need to been cryptic, while the database service provider should be able to efficiently answer queries based on encrypted data and queries."Distributing Data for Secure Database Services,"

V.Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani [9] have proposed, the advent of database services has resulted in privacy concerns on the part of the client storing data with third party database service providers. This paper provide algorithms for (1) distributing data: our results include hardness of approximation results and hence a heuristic greedy algorithm for the distribution problem (2) partitioning the query at the client to queries for the servers is done by a bottom up state based algorithm. Finally the results at the servers are integrated to obtain the answer at the client. "How to Share a Secret," A. Shamir[10], has described how to divide data D into n pieces in such a way that D is easily reconstruct able from any k pieces, but even complete knowledge of k-1 pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when miss fortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

III. THE PROPOSED APPROACH

This structure illustrates in Fig.1 the proposed process contain owner, User, Cloud. Every time owner store the data in encrypted structure using keys.

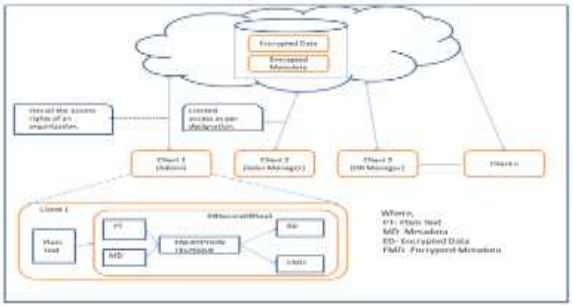

Fig .1. Architecture Diagram

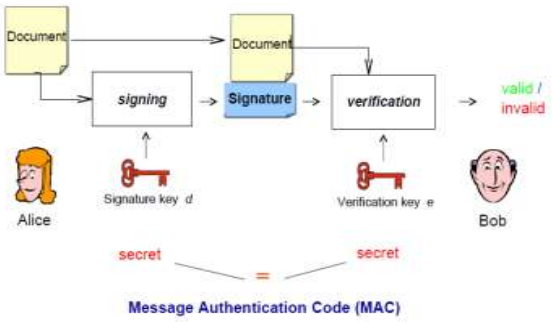

Fig .2 Overall views

TPA is a controller of owner, user and Cloud. The clients are utilizing this method via receiving the message and getting data from Cloud. Cloud data Base is unbiased access between owner and user.

For System Process

User Side

2. Cloud asks User for authentication just like log in 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.

Recently Novell announced support for the Cloud Me service in their Dynamic File Services Suite. Novo soft Handy Backup version 7.3 also announced support for Cloud Me. There are many third party mobile apps and software available for Cloud Me, many using the Web DAV support of Cloud Me.

The users can enhance the usage of Cloud Me through having iPhone or Android mobile. Once Cloud Me is set up on the device, we can with no trouble access the data in all places the network. If the user makes changes within the cloud, then all the specified changes will likely be made to different data as good. For illustration, if a image is involved in CloudMe iPhone application and saved within the CloudMe folder, then it is going to even be available on the PC power as good. CloudMe may also be hooked up on a couple of desktops at the equal time, for illustration, on home and work computer so that we can have the entire files available on both the computers. There is no longer a ought to have a USB-Rimini scene stick with us. Extra, CloudMe enables the person synchronize multiple folders simultaneously. Now that we may maintain our photographs, track, movies and files all equipped with in the same folder as we at all times desired to have however now with a further CloudMe features.

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

An Given a cipher textual content c and a public key (n,e), computing m such that we write it as c≡me mod n .

Mathematical method: Compute an e-th root mod n . Factorization hindrance (within the context of RSA) Given a ordinary quantity n composed of two primes p and q, compute p and q. Attacker is ready to decrypt (or signal), if he is aware of d , Computation of d is at present finished via (p-1). (q-1) , Attacker explanations n, i.e. He computes p and q.

We suggest a enormous safety growth to the using novel architecture that integrates cloud database offerings with data confidentially and the likely hood of executing the concurrent operation on encrypted data. This is the primary answer assisting geographically allotted purchasers to attach instantly to an encrypted cloud data base and to execute concurrent and unbiased operation together with these modifying the database constitution. Secure DbaaS provides several usual facets that differentiate it from prior work in the field of protection for far away database offerings.

The Proposed structure does now not require changes to the cloud database and it's right away relevant to present cloud DBaaS. Such as the experimented postgreSQL plus cloud database, home windows Azure and Xeround. There are no theoretical and realistic limits to extend our options to different structures and to include new encryption algorithm. It guarantees information confidentiality by enabling a cloud database server to execute concurrent SQL operations (not simplest read/write, but additionally adjustments to the database constitution) over encrypted data. It provides the identical availability, elasticity, and scalability of the customary cloud DBaaS considering that it does not require any intermediate server.

IV. CONCLUSION

In this paper now we have proven overheads on storage, communication and the computation of our data. This may occasionally strengthen the efficiency of communiqué and storage security. A revolutionary structure that guarantees confidentiality of data stored in public cloud databases. A massive part of the research entails solutions to help concurrent SQL operations including statements enhancing the database structure on encrypted information issued

by means of heterogeneous and almost certainly geographically dispersed clients. There are not any theoretical and practical limits to lengthen our method to different systems and to comprise new encryption algorithm. It is worth looking that experimental results situated on the TPC-C ordinary benchmark show that the performance have an effect on of data encryption on response time turns into negligible considering that it is masked through community latencies which might be average of cloud scenarios.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing,"Comm. of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W.Felten, "SPORC: Group Collaboration Using UntrustedCloud Resources," Proc. Ninth USENIX Conf.Operating Systems Design and Implementation, Oct.2010.

[3] J. Li, M. Krohn, D. Mazie` res, and D. Shasha, "SecureUntrusted Data Repository (SUNDR)," Proc. SixthUSENIX Conf. Operating Systems Design andImplementation, Oct. 2004.

[4] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M.Dahlin, and M. Walfish, "Depot: Cloud Storage withMinimal Trust", ACMTrans. Computer Systems, vol.29, no. 4, article12, 2011.

[5] H. Hacigu¨ mu¨ s,, B. Iyer, and S. Mehrotra, "ProvidingDatabase as a Service", Proc. 18th IEEE Int'l Conf. DataEng.Feb.2002.

[6] C. Gentry, "Fully Homomorphic Encryption Using IdealLattices", Proc. 41st Ann. ACM Symp. Theory ofComputing May 2009.

[7] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H.Balakrishnan, "CryptDB: Protecting Confidentialitywith Encrypted Query Processing," Proc. 23rd ACMSymp. Operating Systems Principles, Oct. 2011.

[8] J. Li and E. Omiecinski, "Efficiency and Security TradeOff in Supporting Range Queries on EncryptedDatabases," Proc. 19thAnn. IFIP WG 11.3 WorkingConf. Data and Applications Security, Aug. 2005.

[9] V.Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina,and R.Motwani, "Distributing Data for Secure DatabaseServices," Proc. Fourth ACM Int'l Workshop Privacyand Anonymity in the Information Soc., Mar. 2011.

[10] A. Shamir, "How to Share a Secret", Comm. of theACM, vol. 22, no. 11, pp. 612-613, 1979.

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

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

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

Authors:

CHITTIMALLA SOWMYASRI was born in India. She is pursuing M. Tech degree in Computer Science & Engineering in CSE Department in Vaagdevi college Of Engineering, Bollikunta, Warangal Dist Telangana State, India.

Mr. MANYAM SUKESH was born in India in the year of 1989. He received B. Tech degree in the year

of 2010. He was expert in Mobile computing, Computer Organization and architecture, java, DAA. He is currently working as An Asst.Professor in the CSE Department in Vaagdevi College of Engineering, Bollikunta, Warangal, and Telangana State, India.