Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.153 – 157

RESEARCH ARTICLE

Secured Data Transfer Over Cloud Networks

Siddanth Sarathy[1], Ketan Pawar[2], Saurabh Udgirkar[3], Jehan Joshi[4]

[1]Department of Computer Science Savitribai Phule Pune University, India

[2]Department of Computer Science Savitribai Phule Pune University, India

[3]Department of Computer Science Savitribai Phule Pune University, India

[4]Department of Computer Science Savitribai Phule Pune University, India

[1] sid1276@gmail.com; [2] ketan.pv@gmail.com;
[3] saurabhudgirkar.2020@gmail.com; [4] jehanjoshi@gmail.com

Abstract— Cloud computing has the potential to transform a large part of the IT industry by making the software even more attractive and shaping the way in which IT hardware is designed and purchased. Cloud computing means different things to different people. Cloud computing remains a work in progress even though the aspects of these characteristics have been realized to a certain extent. Every user in today's environment wants to access their data at any time and at anywhere. There should be a guarantee of security and availability for data while placing critical data in the hands of a cloud provider. We provide a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. There are two main privacy issues. First issue would be that the owner of the data should be assured that the data stored on the service-provider site is protected against data thefts from outsiders. Second issue would be that the data should be protected even from the service provider, if the providers themselves cannot be trusted.

Keywords— Data Transfer, Cloud Networks, Data confidentiality

I. INTRODUCTION

We hereby have chosen the domain of cloud computing considering the possibilities of further research in this domain, the technology associated with this domain is slowly changing the way data is shared over the network between devices connected over the network this is what intrigued us to carry out further research in this domain and moreover Indian government is considering the possibility of using cloud computing for encrypted data transfer so this gives us a larger scope over this domain as well.

With a fledgling cloud computing market in the country, both Indian and international cloud players are ramping up capacity to meet the increasing demand and are expected to spend over Rs.10000cr in the next three years.

From the perspective of data security, cloud computing poses new challenging security threats for various number of reasons. The data which has been stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering etc.

It is very important to secure store, manage and share data so that any unauthorised person cannot access a data or make changes to it. The data which is named by a person have no control over where his data is accessed. If one wants to take benefits of data is cloud which is not secured than, he can easily use the resource, allocate it and make changes to it. So we have to safeguard the data to secure it from the unauthorised processes. Mostly, the data in the cloud must be encrypted, so that the data must be secured. Data security involves ensuring that appropriate policies are used for sharing the data. Much of the data in cloud must be encrypted by querying encrypted data. In this paper, we are going to show how to secure the data in cloud from the third party. For eg: If a file is generated by a user and it saves in cloud. If owner of file give permission to second user, they owner will allocate key to second user, by using that key the user can make changes to data. Similarly if third party is not allocated a key by owner, he cannot access data till the key is allocated to it. Third party will see data in the encrypted form.

II. RELATED WORK

The architecture design motivated us by three goals: to allow multiple, independent, and geographically distributed clients to execute concurrent operations on encrypted data, which also includes SQL statements that modify the structure of database; to preserve confidential data and consistency at the client and cloud level; to eliminate any intermediative server between the cloud client and the cloud provider.

In order to ensure the dependability and security for data storage in cloud, we aim to design mechanisms which are efficient for dynamic data verification and operation and achieve the following goals:

- Dependability - To enhance availability of data against malicious data modification and server colluding attack.
- Dynamic data support – There should be an assurance that the same level of storage correctness should be maintain even if users modify, append or delete their data files in the cloud.
- Lightweight- Performance of storage correctness checks with minimum overheads should be enabled to the users.
- Storage correctness- To ensure users that their data are stored appropriately and kept intact all the time in the cloud.

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. Response times are affected by cryptographic overheads that for most SQL operations are masked by network latencies.

.Multiple clients, possibly geographically distributed, can access concurrently and independently a cloud database service.

It does not require a trusted broker or a trusted proxy because tenant data and metadata stored by the cloud database are always encrypted.

It is compatible with the most popular relational database servers, and it is applicable to different DBMS implementations because all adopted solutions are database agnostic.

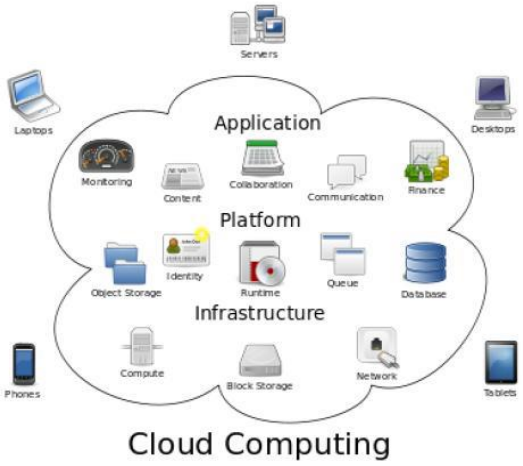

Figure 1: Cloud Computing

Some techniques we bring into account for the security of data and reliability of data are as follows:

Reverse Circle Cipher: This technique is used to ensure data security as well as network security. This technique reduces time and space complexity both by using circular substitution. It optimizes performance of data and also provides high level of security to data. This technique is proved as a very difficult cipher to break by the experimentalist.

Key Generation: It is a process in which the key is generated by the owner of data in order to allocate this key to a person whom he want to make changes to data. A key is used to encrypt as well as decrypt data. To read encrypted data "brute force attack" method is used. In this method, every number is attempted as long as the length of key. Thus the length of key must be maximum.

Key Distribution: Key distribution is more complicated in cloud. "Secret Sharing" technique is used for key distribution and key storage at many different servers on the cloud. In Secret Sharing technique, some private things are used as a hint from which many different private things can be generated and these things are distributed in such a manner that some part of those things can easily authenticate themselves and use private data without knowing what it is. The key is distributed to the authorized users and by using private shares which is stored at multiple locations in such a manner that these subset will be useful for again generation of key.

Key Management: In cloud, it is a process in which initially the resource is selected from cloud. The next step is to get accessibility for that resource from the owner of that resource. The accessing hierarchy is checked further and then the key allocated is used and resource can be modified further.

III. SYSTEM ARCHITECTURE

Secure DBaaS is designed to allow various clients from local machines to connect directly to the untrusted cloud DBaaS without any specific authentication. We consider that a tenant organization gets cloud database services from an untrusted provider. The tenant then establish one or more machines (Client 1 through N) and installs a Secure DBaaS client on SQL statements, each plaintext table is converted into a secure table because the cloud database is untrusted. The name of a secure table is obtained by encrypting the name of the belonging plaintext table. The data type represents the type of the plaintext data(e.g., int, varchar). The encryption type identifies the encryption algorithm that is used to cipher all the data of a column.

The field confidentiality parameter allows a tenant to define explicitly which columns of which secure table and the unencrypted name of the related plain text table. Moreover, table metadata include column metadata for each column of the related secure table. Each column metadata contain the following information.

• **Plain name**: the name of the corresponding column of the plain text table.

• **Coded name**: the name of the column of the secure table. This is the only information that links a column to the corresponding plaintext column because column names of secure tables are randomly generated.

• **Secure type**: the This allows a Secure DBaaS client to be informed about the data type and the encryption policies associated with a column.

• **Encryption key**: the key used to encrypt and decrypt all the data stored in the column.

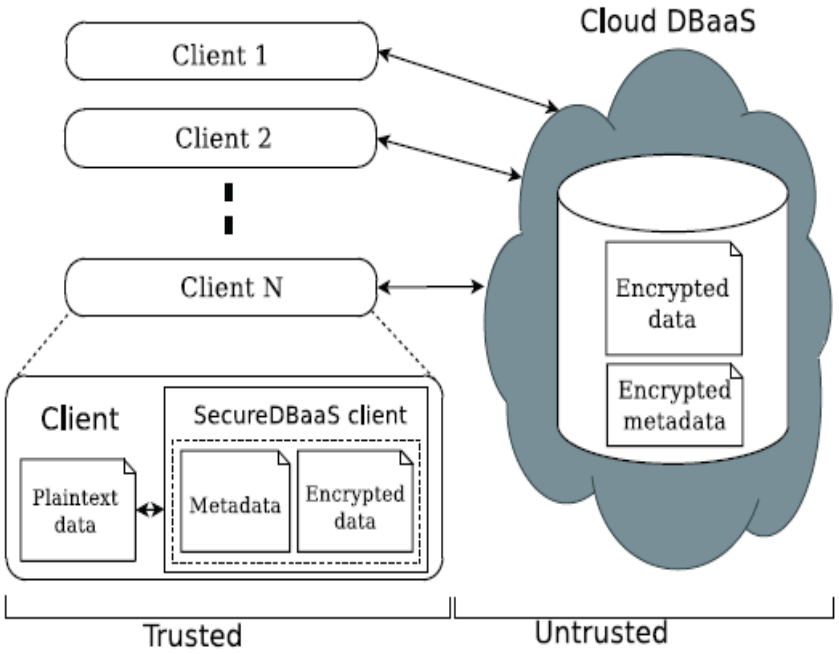

Figure 2 : Secure DBaaS architecture.

IV. CONCLUSION

Here, we investigated the problem of data security in cloud data storage and data transfer, which is essentially a distributed storage system. We propose an architecture that guarantees data confidentiality 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 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. There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithms.

ACKNOWLEDGEMENT

We would like to express the deepest appreciation to our guide Prof. Rupesh Mahajan and our Head of Department Prof. Pramod Patil. We thank our parents who have been shown tremendous support and inspired us with their blessings. We would like to express our gratitude with a word of thanks to all of those who have directly or indirectly helped us by giving beneficial information and knowledge.

REFERENCES

[1] Luca Ferretti, Michele Colajanni, and MircoMarchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.

[2] PradnyeshBhisikar **,**Prof. AmitSahu **,** Security in Data Storage and Transmission in Cloud Computing, Volume 3, March 2013, International Journal of Advanced Research in Computer Science and Software Engineering

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

[4] W. Jansen and T. Grance" Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication 800-144, NIST, 2011.

[5] 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.

[6] D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, "Database Management as a Service: Challenges and Opportunities," Proc. 25th IEEE Int'l Conf. Data Eng., Mar.-Apr. 2009.

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

[8] 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.

[9] QianWang, Cong Wang, KuiRen, Wenjing Lou Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011.

[10] "Security and Privacy Challenges in Cloud Computing Environments" co-published by the IEEE computer and reliability ieee november/december2010.

