Volume 6, Issue 9, September 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study on the Techniques for Distributed Stored Data Security in Cloud Computing

Dr. P. Julia Grace, Ph.D.
Assistant Professor and Research Supervisor
Department of Computer Science
JBAS College for Women, Chennai, India

A. Rachel Rathna Sheela
M. Phil. Computer Science Scholar
Mother Teresa Women's University Extn. Center,
Saidapet, Chennai, India

Abstract: ***Cloud Computing has gained great attention from both industry and academia since a decade. This paper deals with the basic concepts of cloud computing and proposes two methods - one for file sharing system and other for non-file sharing system. Using distributed Storage, it reduces the load of an owner in maintaining enormous number of files. It reduces time, ensures data integrity and takes care of shared files via Cloud; thereby disambiguation of data can be avoided.***

Keywords: Cloud, File sharing, TDB.

I. INTRODUCTION

Cloud computing is an innovative technology that is revolutionizing the way we do computing. It is a buzzword that means different things to different people. For some, it is just another way of describing IT (information technology) "outsourcing"; others use it to mean any computing service provided over the Internet or a similar network. The goal of cloud computing is to reduce time spending on technology infrastructure, globalizing workspace and easy accessibility, better resource utilization, improving scalability, backup and disaster recovery and many more. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems which are linked together. The basic structure of Cloud computing is shown in fig. 1.1.

Few notable benefits to cloud consumers include:

- On-demand access to pay-as-you-go computing resources on a short-term basis (such as processors by the hour), and the ability to release these computing resources when they are no longer needed.
- The perception of having unlimited computing resources that are available on demand, thereby reducing the need to prepare for provisioning.
- The ability to add or remove IT resources at a fine-grained level, such as modifying available storage disk space by single gigabyte increments.
- Abstraction of the infrastructure so applications are not locked into devices or locations and can be easily moved if needed.

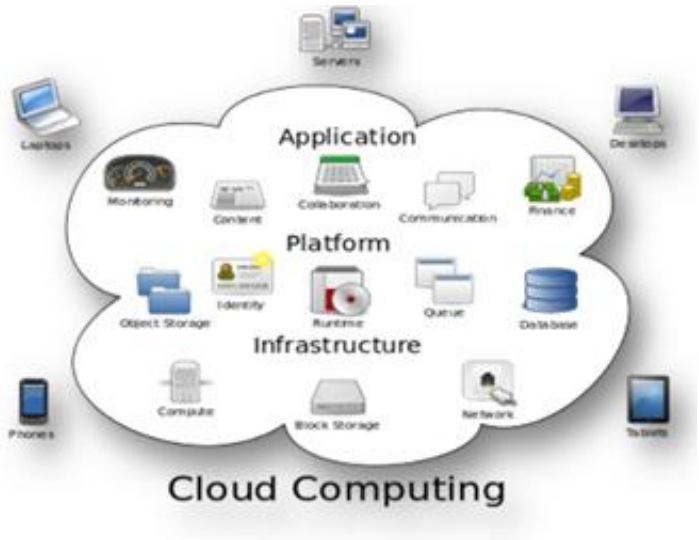

Fig. 1.1. *Basic* Structure of cloud computing

II. SERVICES MODELS

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure 2.1. If a cloud user accesses services on the infrastructure layer, for instance, they can run their own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If they accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

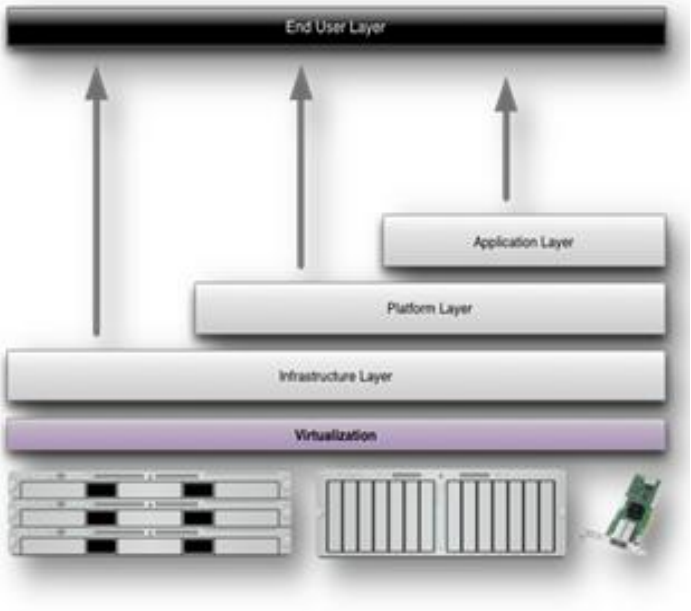

Fig 2.1. Structure of service Models

III. IMPLEMENTATION

There are four modules: Data Owner, Private key Generator, Proxy Server and the Receiver Module.

3.1. Data Owner:

In this module, first the new data owner registers and then get a valid login credentials. After logged in, the data owner has the permission to upload their file into the Cloud Server. The data owner encrypts his data and outsources the cipher texts to the proxy servers.

3.2. Private Key Generator:

In this module, the private key generator (PKG) validates the users' identities and issues secret keys to them. The key is generated and sent to their respective mail id's with the file name and the corresponding key values.

3.3. Proxy Server:

In computer networks, a proxy server is a server, that acts as an intermediary for requests from clients seeking resources from other servers.

Proxy servers store the encrypted data and transfer the cipher text for the owner to the cipher text for the receiver when they obtain access permission (re-encryption key) from the owner. In these systems, proxy servers are assumed to be trusted. They authenticate receivers and validate access permissions. The interactions between the proxy servers and receivers are executed in a secure channel. Therefore, these systems cannot provide an end-to-end data security and they cannot ensure the confidentiality of the data stored at the proxy server. In these data sharing, a receiver authenticates himself to the proxy server using his password. Then, the proxy server passes the authentication result to the file owner. The owner will make access permission according to the received information.

3.4. Receiver Module:

The receiver authenticates himself to the owner and decrypts the re-encrypted Cipher text to obtain the data. In these systems, an end to-end security is provided by cryptographic protocols which are executed by the file owner to prevent proxy servers and unauthorized users from modifying and accessing the sensitive files. These systems can be divided into two types: shared file system and non-shared file system. In shared file systems the owner can share his files with a group of users. Cryptographic techniques deployed in these systems has the concept of key sharing, key agreement and key revocation. In non-shared file systems in order to share a file with another user, the owner can compute an access key for the user using his secret key. In these two systems, the integrity of the sensitive files is provided by digital signature data sharing and message authentication codes (MAC).

IV. DISTRIBUTED STORED SECURITY CONCEPTS

At first, the owner of the data needs to be assured that the data stored on the service-provider site is protected against data thefts from outsiders. Secondly, data needs to be protected even from the service providers as the providers themselves cannot be trusted. In this paper, we focus on the second aspect. Specifically, we explore few techniques to execute SQL queries over encrypted data. Our strategy is to process as many queries as possible at the service providers' site, without having to decrypt the data. Decryption and the remainder of the query processing are performed at the client site and explores an algebraic framework to split the query to minimize the computation at the client site. A sample result of the experiments validating our approach is illustrated in fig 4.1.

(Fig.4.1. Encrypted File under data owner)

The database is encrypted and validated against a collision-resistant hash kept in trusted storage, so untrusted programs cannot read the database or modify it undetectably. Trusted database system (TDB) integrates encryption and hashing with a low-level data model, which protects data and metadata uniformly, unlike systems built on top of a conventional database system. The implementation exploits synergies between hashing and log-structured storage. Preliminary performance results show that TDB outperforms an off-the-shelf embedded database system, thus supporting the suitability of the TDB architecture.

V. CONCLUSION

Stored data security technique allows the third party to outsource their files to untrusted proxy servers via cloud with a secured distributed data sharing. Using this, the users are identified by their identities and can communicate without the need of verifying the public key certificates. The file owner can decide access permission independently for each file. In non-shared files system, a user can access only one file for a single query and in shared file system, they can access multiple groups; thereby ambiguity of data can be avoided.

REFERENCES

[1] H. Hacig¨um¨us, B. R. Iyer, C. Li, and S. Mehrotra, “Executing SQL over encrypted data in the database-service-provider model,” in Proceedings: SIGMOD Conference - SIGMOD’02 (M. J. Franklin, B. Moon, and A. Ailamaki, eds.), vol. 2002, (Madison, Wisconsin, USA), pp. 216–227, ACM, Jun. 2002.

[2] L. Bouganim and P. Pucheral, “Chip-secured data access: Confidential data on untrusted servers,” in Proc. International Conference on Very Large Data Bases - VLDB’02, (Hong Kong, China), pp. 131– 142, Morgan Kaufmann, Aug. 2002.

[3] U. Maheshwari, R. Vingralek, and W. Shapiro, “How to build a trusted database system on untrusted storage,” in Proc. Symposium on Operating System Design and Implementation - OSDI’00, (San Diego, California, USA), pp. 135–150, USENIX, Oct. 2000.

[4] A. Ivan and Y. Dodis, “Proxy cryptography revisited,” in Proc. Network and Distributed System Security Symposium - NDSS’03, (San Diego, California, USA), pp. 1–20, The Internet Society, Feb. 2003.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption data sharing with applications to secure distributed storage,” in Proc. Network and Distributed System Security Symposium - NDSS’05, (San Diego, California, USA), pp. 1–15, The Internet Society, Feb. 2005.

AUTHORS PROFILE

Dr. (Mrs.) Julia Grace P., received her B.Sc., Computer Science in 2000 and MCA in 2003, both from Manonmaniam Sundaranar University. She got the University FIRST Rank in MCA. She got her B.Ed., in 2004 from University of Madras, M.Phil., from Madruai Kamaraj University in 2005 and Ph.D. from Mother Teresa Women's University in 2013. Presently, she is working as Assistant Professor in Computer Science in JBAS College of Women (Autonomous), Chennai. Till Date, she has guided 12 M.Phil. Scholars, presented 14 papers in National, International Conferences and published 12 research articles in International Journals. Her areas of interest are Artificial Intelligence, System Biology, Machine Learning and Theoretical Computer Science. She is a life member of International Association of Professional Academicians, members of International Association of Engineers, executive board member and review member for few reputed Journals.

Mrs. Rachel Rathna Sheela. A is currently doing M.Phil., Computer Science in Mother Teresa Women's University, Chennai Centre, after her MCA in June 2012.

