

{tag} International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

[Volume 148](#)

-
[Number 12](#)

Year of Publication: 2016

Authors:

Jadhav Sonali S., B. M. Patil

10.5120/ijca2016911323

{bibtex}2016911323.bib{/bibtex}

Abstract

In today's environment the various vital information should need to be stored in more secured manner. In the cloud computing, original plain data must be accessible only by trusted parties that do not include internet and cloud providers or intermediaries. Storing this confidential information in cloud must provide guarantee of availability of data and security. there are too many solutions are provided to handle data, but still confidentiality problem is at risk. For that reason in this work proposed a new novel architecture SecureDBaaS which provides confidentiality and as well as allows concurrent execution of operations on encrypted data with distributed policy also. SecureDBaaS architecture retrieves the necessary information or metadata through SQL processing. This architecture has advantage that eliminates the intermediate server between client and cloud database also modifies the database structure. It guarantees for data confidentiality by performing SQL operations over encrypted cloud databases. This intended result of the proposed architecture is evaluated through comparison of AES n DES algorithm, where AES is better than DES is proved by studying comparison results.

References

1. M. Armbrust et al., "A View of Cloud Computing," *Comm. of the ACM*, vol. 53, no. 4, pp. 50-58, 2010.
2. W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication 800-144, NIST, 2011.
3. 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..
4. J. Li, M. Krohn, D. Mazieres, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," *Proc. Sixth USENIX Conf. Operating Systems Design and Implementation*, Oct. 2004.
5. P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud Storage with Minimal Trust," *ACM Trans. Computer Systems*, vol. 29, no. 4, article 12, 2011.
6. H. Hacigu"mu" s., B. Iyer, and S. Mehrotra, "Providing Database as a Service," *Proc. 18th IEEE Int'l Conf. Data Eng.*, Feb. 2002.
7. C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," *Proc. 41st Ann. ACM Symp. Theory of Computing*, May 2009.
8. R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," *Proc. 23rd ACM Symp. Operating Systems Principles*, Oct. 2011.
9. H. Hacigu"mu" s., B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," *Proc. ACM SIGMOD Int'l Conf. Management Data*, June 2002.
10. 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.
11. E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," *Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security*, July/Aug 2006.
12. 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.
13. A. Shamir, "How to Share a Secret," *Comm. of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.
14. "Oracle Advanced Security," Oracle Corporation, <http://www.oracle.com/technetwork/database/options/advanced-security>, Apr. 2013.
15. G. Cattaneo, L. Catuogno, A.D. Sorbo, and P. Persiano, "The Design and Implementation of a Transparent Cryptographic File System For Unix," *Proc. FREENIX Track: 2001 USENIX Ann. Technical Conf.*, Apr. 2001.
16. E. Damiani, S.D.C. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Balancing Confidentiality and Efficiency in Untrusted Relational Dbms," *Proc. Tenth ACM Conf. Computer and Comm. Security*, Oct. 2003.
17. L. Ferretti, M. Colajanni, and M. Marchetti, "Supporting Security and Consistency for Cloud Database," *Proc. Fourth Int'l Symp. Cyberspace Safety and Security*, Dec. 2012.
18. "Transaction Processing Performance Council," TPC-C, <http://www.tpc.org>, Apr. 2013.

19. Xeround: The Cloud Database,” Xeround, <http://xeround.com>, Apr. 2013.
20. “Postgres Plus Cloud Database,” EnterpriseDB, <http://enterprisedb.com/cloud-database>, Apr. 2013.
21. 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, February 2014

Index Terms

Computer Science

Information Sciences

Keywords

SecureDBaaS, cloud, security, DBaaS