A Hybrid Cryptographic Technique for Secured Authentication in Cloud Computing

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

Volume 141 - Number 13

Year of Publication: 2016

Authors:
Juber Mirza, Meena Sharma

10.5120/ijca2016909797

Abstract

The cloud infrastructure development and service distribution is a complex task. A number of members are contributing in this task such as clients, intermediate service providers and the data centre owners. In such kind of scenarios the infrastructure providers are distribute their service by the help of intermediate servers or vendors. Due to this the quality of service, trust, security and privacy of the data and their owner is a key issue of management. Therefore a secure and trust worthy environment is need to be created for improving the data owner trust on the primary service providers.

In this presented work the key focus of the study is placed on the server security and the user trust management. Therefore the proposed technique involves the development of secure cryptographic cloud. The cryptographic cloud is implemented with the help of a hybrid cryptographic technique which involve the Data Encryption standard (DES) encryption technique for ciphering data and for key exchange the Diffie Hellman (DH) algorithm is implemented. Further for more improved security the integrity check is also implemented with
the help of Message Digest (MD) 5 hash generation algorithm. After implementation of the
contextographic cloud the trust management between the primary service provider and brokers
are need to implement for managing the end client trust on primary service provider. Therefore
a two factor trust computation technique is proposed using the server rating and the number of
request failures. This trust value is help to regulate the quality of service offered by the primary
service provider.

The implementation of the proposed technique is performed with the help of JAVA technology
and their performance is reported with the help of space and time complexity. According to the
experimental results the proposed technique offers more secure environment and with less
computational overheads.

References

1. Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, Jinjun Chen, “MuR-DPA:
   Top-down Levelled Multi- replicaMerkle Hash Tree Based Secure Public Auditing for Dynamic
   Big Data Storage on Cloud”, IEEE Transactions on Computers (Volume:64 , Issue: 9)
   of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified
   Conference on Advances in Computer Science and Applications with International Journal of
   Computer Applications (NCACSA 2012)
5. MilenkoRadonic, “Cloud vs. Data Center: What's the difference”,
   http://www.glbrain.com/index.php?r=tool/view&id=2103&toolType=1
   Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622International
   Conference on Humming Bird (01st March 2014)
7. SwapnaLia Anil, RoshniThanka, “A Survey on Security of Data outsourcing in Cloud”,
   Storage”, International Journal of Computer Applications (0975 – 8887) Volume 120 – No.5,
   June 2015
   University of Helsinki, Finland, 20th of October 2001
10. Sheikh MahbubHabib, Sebastian Ries, Max Muhlhauser, “Towards a Trust Management
    System for Cloud Computing”, 2011 IEEE 10th International Conference on Trust, Security and
    Privacy in Computing and Communications (TrustCom)
11. Kai Hwang, Deyi Li, “Trusted Cloud Computing with Secure Resources and Data
    Colouring”, Published by the IEEE Computer Society, 1089-7801/10/$26.00 © 2010 IEEE, IEEE
    Internet Computing
12. Sidhu and Sarbjeet Singh, “Compliance based trustworthiness calculation mechanism in
    cloud environment”, International Workshop on Intelligent Techniques in Distributed Systems


**Index Terms**

Computer Science  
Information Sciences

**Keywords**

Cloud Security, Trustworthy Cloud, Privacy on Cloud, Secure Cryptographic Cloud, Transparency