IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

How Homomorphic Cryptosystem used for Cloud Database

Kedar S. Yele[1] and Mr. Prakash Sakharkar[2]
Student, Department of MCA[1]
Professor, Department of MCA[2]
Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application, Mumbai, India
kedaryele0@gmal.com

Abstract: *The concept of cloud computing receiving a great deal of attention both in publication and among users. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware resources that are managed by cloud providers at remote locations. The distance between the client and the physical location of his data creates a barrier because this data can be accessed by a third party and this would affect the privacy of client's data. The using of traditional encryption schemes to encrypt the remote data before sending to the cloud provider has been most widely used technique to bridge this security gab. But, the client will need to provide the private key to the server to decrypt the data before perform the calculations required. Homomorphic encryption allows performing computations on encrypted data without decryption. This paper deals with the use of homomorphic encryption to encrypt the client's data in cloud server and also it enables to execute required computations on this encrypted data.*

Keywords: Homomorphic encryption

REFERENCES

[1]. P. Mell, T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U. S. Department of Commerce, (2011).
[2]. J. Li, D. Song, S. Chen, X. Lu, "A Simple Fully Homomorphic Encryption Scheme Available in Cloud Computing", In Proceeding of IEEE, (2012).
[3]. M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, "Fully homomorphic encryption over the Integers", in Proceedings of Advances in Cryptology, EUROCRYPT'10, pages 24–43, 2010