تاریخچه مقاله:

تاریخ ارسال: ۹۸/۰۹/۱۰
تاریخ اصلاحات: ۹۸/۱۱/۱۲
تاریخ پذیرش: ۹۸/۱۲/۱۵
تاریخ انتشار: ۹۸/۱۲/۲۰

Keywords:

Cloud Computing
Security
Privacy-Preserving
Additive Homomorphic
Order-Preserving
Scheme.

Lightweight Additive Homomorphic Schemes for Cloud Outsourcing Scenarios

Somayeh Sobati.M[1]*
[1] Hakim Sabzevari University, Sabzevar, Iran

Abstract

Data privacy is a major concern in a cloud computing environment that uses the Database-as-a-Service model. Nevertheless, the existing encryption schemes are only partly homomorphic and are designed to enable for one particular method of computation to be carried out on encrypted data. To address these concerns, we have recently proposed new partially homomorphic schemes that preserve data privacy in a cloud database while still enabling encrypted data to be processed. The proposed schemes allow the processing of queries with an order-preserving partial homomorphic encryption scheme. We've shown that our schemes are a realistic framework that protect data privacy with reduced overhead.

روش ارجاع به مقاله:

S.Sobati.M, Lightweight Additive Homomorphic Schemes for Cloud Outsourcing Scenarios, Journal of Distributed Computing and Systems (JDCS) Vol.2, No.2, PP.170-177, 2020

Email: s.sobati@hsu.ac.ir