CORE
Metadata, citation and similar papers at core.ac.uk
Provided by UMS Institutional Repository

Securing Big Data Processing With Homomorphic Encryption

ABSTRACT

The arrival of Big Data era has challenged the conventional end-to-end data protection mechanism due to its associated high volume, velocity and variety characteristics. This paper reviews the security mechanisms of dominated Big Data processing platform – Hadoop and examines its capabilities on providing the end-to-end data protection: data-in-transit, data-at-rest and data-in-transform. While Hadoop is limited to protect data-in-transit with its built-in security mechanism and relies on third-party vendor tools (e.g. HDFS disk level encryption or security-enhanced Hadoop security distribution) for securing data-at-rest, the homomorphic encryption scheme that capable of performing computation on encrypted data serve as a promising tool to provide end-to-end data protection Big Data processing. However, existing circuit-based homomorphic encryption schemes still insufficient enough for supporting Big Data applications due to their high complexity of computation, huge generated ciphertext and public key size. To address this problem, this paper proposed homomorphic encryption from a non-circuit-based approach. Our result shows that the newly proposed non-circuit based homomorphic encryption has greatly reduced the computation time and ciphertext size as compared to existing circuit-based homomorphic encryption schemes, therefore amenable to support the high volume and high-velocity requirement of Big Data processing.