A survey of homomorphic encryption for outsourced big data

ABSTRACT

With traditional data storage solutions becoming too expensive and cumbersome to support Big Data processing, enterprises are now starting to outsource their data requirements to third parties, such as cloud service providers. However, this outsourced initiative introduces a number of security and privacy concerns. In this paper, homomorphic encryption is suggested as a mechanism to protect the confidentiality and privacy of outsourced data, while at the same time allowing third parties to perform computation on encrypted data. This paper also discusses the challenges of Big Data processing protection and highlights its differences from traditional data protection. Existing works on homomorphic encryption are technically reviewed and compared in terms of their encryption scheme, homomorphism classification, algorithm design, noise management, and security assumption. Finally, this paper discusses the current implementation, challenges, and future direction towards a practical homomorphic encryption scheme for securing outsourced Big Data computation.