Ph: 9585554590, 9585554599
Email: support@salemsmartreach.com
URL: www.salemsmartreach.com

On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage

Abstract:

Provable data possession (PDP) is a probabilistic proof technique for cloud service providers (CSPs) to prove the clients' data integrity without downloading the whole data. In 2012, Zhu et al. proposed the construction of an efficient PDP scheme for multicloud storage. They studied the existence of multiple CSPs to cooperatively store and maintain the clients' data. Then, based on homomorphic verifiable response and hash index hierarchy, they presented a cooperative PDP (CPDP) scheme from the bilinear pairings. They claimed that their scheme satisfied the security property of knowledge soundness. It is regretful that this comment shows that any malicious CSP or the malicious organizer (O) can generate the valid response which can pass the verification even if they have deleted all the stored data, i.e., Zhu et al.'s CPDP scheme cannot satisfy the property of knowledge soundness. Then, we discuss the origin and severity of the security flaws. It implies that the attacker can get the pay without storing the clients' data. It is important to clarify the scientific fact to design more secure and practical CPDP scheme in Zhu et al.'s system architecture and security model.