Abstract

Wireless body area network (WBAN) is composed of sensors that capture and transmit physiological data to an application provider's (AP) remote server. When integrated into the Internet of Things (IoT) infrastructure, WBAN data can be accessed from anywhere and at anytime. A secure storage and access mechanism to this sensitive data is necessary within a heterogeneous IoT. Searchable encryption (SE) provides secure method that could be used by an AP for example, hospital employees to securely access a patient's medical record. This is achieved by sending a trapdoor function to remote server. In this paper, we propose a new SE technique based on a signcrypted keyword and a designated tester. It is constructed from Li et al.'s practical signcryption scheme. In the proposed scheme, a data owner (WBAN) operates in certificateless cryptography, while a designated tester (server) and a receiver are both in public key infrastructure environment. We use both authenticity and confidentiality property of a signcryption scheme to proof that our scheme is provably secure against keyword guessing attack. A quantitative analysis on performance against other certificateless SE schemes shows that our scheme is computationally lightweight during keyword-ciphertext and trapdoor generation.