Abstract

A multi-server environment is an important application paradigm in the Internet of Things (IoT). It enables a user access services from different vendors without having to go through multiple registration. The privacy of one who desires to access these services is often crucial. In order to access this service in a manner that assures user privacy, a user needs to be anonymously authenticated independent of the vendors' services. However, existing identity-based anonymous schemes are only suitable for the client-server domain. Moreover, these schemes provide conditional anonymity which presupposes that if an adversary discovers the user's private key, the identity can easily be recovered and misused. To avoid this situation, a new unconditional anonymity identity-based user authenticated key agreement scheme for IoT multi-server environment is introduced in this paper. Our protocol applies a ring signature to allow users to anonymously authenticate themselves in the severs without revealing their identities. Hence, an adversary cannot recover the user's identity even when the user's private key is known. We further provide a security proof in the random oracle model. Compared with the existing protocols, our proposed scheme is well fitting for mobile phone applications and guarantees the privacy of users in IoT multi-server domain.