Abstract

Wireless body area network (WBAN) provides a medium through which physiological information could be harvested and transmitted to application provider (AP) in real time. Integrating WBAN in a heterogeneous Internet of Things (IoT) ecosystem would enable an AP to monitor patients from anywhere and at anytime. However, the IoT roadmap of interconnected ‘Things’ is still faced with many challenges. One of the challenges in healthcare is security and privacy of streamed medical data from heterogeneously networked devices. In this paper, we first propose a heterogeneous signcryption scheme where a sender is in a certificateless cryptographic (CLC) environment while a receiver is in identity-based cryptographic (IBC) environment. We then use this scheme to design a heterogeneous access control protocol. Formal security proof for indistinguishability against adaptive chosen ciphertext attack and unforgeability against adaptive chosen message attack in random oracle model is presented. In comparison with some of the existing access control schemes, our scheme has lower computation and communication cost.