

Abstract

With the current advancement in technology, the use of Wireless Body Area Networks (WBANs) has become popular in the healthcare management. They provide a mechanism to collect and transmit physiological data to healthcare providers in remote locations. With the need to secure healthcare data becoming a global concern, mechanisms must be put in place to ensure secure communication of physiological data collected in WBANs. This paper, presents a new authentication scheme for WBANs based on Elliptic Curve Cryptography. Sensor nodes used in WBANs are resource constraint and for that reason, the proposed scheme is both certificateless and pairing-free. We compared the efficiency of our proposed authentication scheme with other related schemes and found that our scheme had considerable efficiency in terms of communication cost and running time.