Abstract

Wireless body area network (WBAN) provide a mechanism of transmitting a persons physiological data to application providers e.g. hospital. Given the limited range of connectivity associated with WBAN, an intermediate portable device e.g. smartphone, placed within WBAN's connectivity, forwards the data to a remote server. This data, if not protected from an unauthorized access and modification may be lead to poor diagnosis. In order to ensure security and privacy between WBAN and a server at the application provider, several authentication schemes have been proposed. Recently, Wang and Zhang proposed an authentication scheme for WBAN using bilinear pairing. However, in their scheme, an application provider could easily impersonate a client. In order to overcome this weakness, we propose an efficient remote authentication scheme for WBAN. In terms of performance, our scheme can not only provide a malicious insider security, but also reduce running time of WBAN (client) by 51 % as compared to Wang and Zhang scheme.