Abstract

M-healthcare applications make use of Body Sensor Network nodes to capture health data from a patient, transfer the data via blue tooth to the patient's smartphone, which in turn transmits the information via a 3G network to remote servers at a Healthcare Center.This paper proposes a group signature authentication scheme composed of a medical users group and a medical personnel group to be used by patients and doctors respectively in the event that during an emergency the battery power of the patient under emergency runs low by using opportunistic computing approach. The group signature authentication scheme which is based on an RSA variant ensures that the privacy of the health information is controlled by the user, while a symptom matching scheme is used to control privacy. The scheme ensures user centric privacy of patient's health information. A detailed security analysis shows that the proposed scheme can withstand several kinds of attacks while at the same time achieving user centered privacy access control. In addition, extensive performance evaluations using simulations on real world maps demonstrate the efficiency and effectiveness in terms of providing high reliable PHI processing and transmission while minimizing the privacy disclosure during and m-Healthcare emergency.