**CONCLUSIONS**

In this paper, we have proposed PPDT, which enables privacy-preserving decision tree classification for health monitoring systems. Different from existing schemes, PPDT transforms a decision tree classifier to boolean vectors, and utilizes symmetric encryption to protect the data privacy. With such a design, PPDT extremely boosts the computation, communication, and storage efficiency. We haveformulated a leakage function L, provided the adaptively L-security definition, and given a simulation-based security proof for PPDT. Performance analyses demonstrate that PPDT achieves O(1) computational complexity with polynomial size indexes. Experimental evaluations demonstrate that PPDT achieves microsecond-level execution time, kilobyte-level communication costs, and kilobyte-level storage costs on Breast-Cancer-Wisconsin dataset. Consequently, we have addressed both the confidentiality and efficiency challenges simultaneously, and PPDT is an efficient, practical, and real-time solution for health monitoring systems. For the future works, we will design a privacy-preserving decision tree classification scheme against malicious adversaries.