Abstract

With the increasing popularity of pervasive devices such as smartphones, Body Sensor Network(BSN), Internet-of-Things devices and cloud computing, mobile eHealthcare has become a research trend in recent years. Disease detection using big data analytics techniques is a popular eHealthcare research focus. However, the disease detection still faces many challenges on privacy of users' sensitive personal information, confidentiality of health service provider's diagnosis model, accuracy of the diagnosis result, efficiency of the query result, etc. In this thesis, we aim to improve the security and privacy performance of the eHealthcare systems, while achieving efficient disease detection.

Firstly, we propose an efficient privacy-preserving pre-clinical guidance service scheme (PGuide) to provide on-the-go medical guidance service while preserving user privacy to address the above-mentioned privacy challenges, improve the accuracy of disease risk in hospitals. Using the PGuide scheme, users can personally conduct privacy-preserving pre-clinical diagnosis based on their health profiles and obtain recommendation from trusted sources (e.g. hospitals and medical service providers) based on the diagnosis. In addition, the information transmitted to the hospitals and other medical service providers to calculate the disease risk use a disease prediction model in a privacy-preserving way.

Secondly, we propose an efficient privacy-preserving health query scheme over outsourced cloud (HeOC). In this scheme, the user filters out the suspicious disease with the sensor collected data first. Then through a variant of oblivious pseudorandom function protocol protocol (OPRF), the user can query the accurate disease level from the filtered result using sensor anomaly detection technique. To reduce the query latency, we propose a novel sensor anomaly detection technique (SADS) for detecting high-risk disease. In the SADS technique, the health service provider outsources an encrypted health tree for reference to the

cloud. Authenticated users send encrypted physiological data to the cloud to detect high-risk disease without disclosing his/her sensitive personal health data. Then, with the oblivious pseudorandom function protocol (OPRF), the user queries the diagnosis result accurately.

Thirdly, we propose an efficient and privacy-preserving priority classification scheme (PPC), for classifying patients' encrypted data at the Wireless Body Area Network gateway (WBAN-gateway) in a remote eHealthcare system. Specifically, to reduce the system latency, we design a non-interactive privacy-preserving priority classification algorithm, which allows the WBAN-gateway to conduct the privacy-preserving priority classification for the received users' medical packets by itself and relay these packets according to their priorities (criticalities).

List of Author's Publications

Journal papers:

[1] G.Wang, R.Lu, and Y.L.Guan, "Enabling efficient and privacy-preserving health query over outsourced cloud", *IEEE Access*, vol. PP, pp. 11, 11 2018.

[1] G.Wang, R.Lu,and Y.L.Guan,"Achieve privacy-preserving priority classification on pa- tient health data in remote eHealthcare system", *IEEE Access*, pp. 1-1, 1 2019.

Conference papers:

[1] G.Wang, R.Lu, C.Huang, "PGuide: An Efficient and Privacy-Preserving Smartphone- Based Pre-Clinical Guidance Scheme", *IEEE*

Globecom'15, San Diego, CA, USA, December 6 - 10, 2015.

[2] G.Wang, R.Lu, C.Huang, "PSLP: Privacy-Preserving Single-Layer Perceptron Learn- ing for e-Healthcare", *ICICS'15*, Singapore, December 2 - 4, 2015.