PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems

Entao Luo[1], Md Zakirul Alam Bhuiyan[2,3], Guojun Wang[3], Md Arafatur Rahman[4], Jie Wu[5], and Mohammed Atiquzzaman[6]
[1]Hunan University of Science and Engineering; [2]Fordham University; [3]Guangzhou University; [4]University Malaysia Pahang; [5]Temple University; [6]University of Oklahoma

ABSTRACT

In IoT-based healthcare, medical devices are more vulnerable to numerous security threats and attacks than other network devices. Current solutions are able to provide protection to patients' data during data transmission to some extent, but cannot prevent some sophisticated threats and attacks such as collusion attacks and data leakage. In this article, we first investigate the challenges with privacy protected data collection. Then we propose a practical framework called PrivacyProtector, patient privacy protected data collection,with the objective of preventing these types of attacks. PrivacyProtector includes the ideas of secret sharing and share repairing (in case of data loss or compromise) for patients' data privacy. Since it is the first time, we apply the Slepian- Wolf-coding-based secret sharing (SW-SSS) PrivacyProtector. In the framework, we use a distributed database consisting of multiple cloud servers, which ensures that the privacy of patients' personal data can remain protected as long as one of the servers remains uncompromised. We also present a patient access control scheme in which multiple cloud servers collaborate in shared construction to offer patients' data to healthcare providers without revealing the content of the data. The privacy performance analysis has shown that the PrivacyProtector framework is secure and privacy-protected against various attacks.

KEYWORDS: Cryptography; Servers; Medical services; Data privacy; Maintenance engineering; Internet of Things