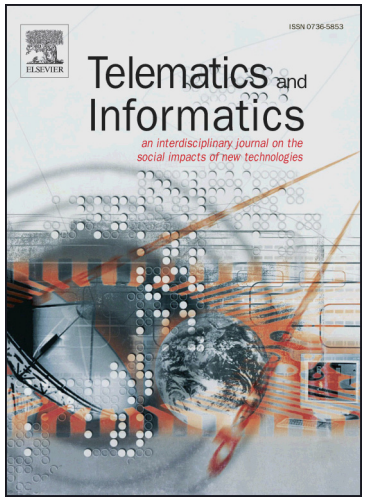

A Trustworthy System for Secure Access to Patient Centric Sensitive Information

Navroop Kaur, Yachana, Sandeep K. Sood

PII: S0736-5853(16)30482-8
DOI: https://doi.org/10.1016/j.tele.2017.09.008
Reference: TELE 1003

To appear in: *Telematics and Informatics*

Received Date: 29 September 2016
Revised Date: 13 August 2017
Accepted Date: 26 September 2017

Please cite this article as: Kaur, N., Yachana, Sood, S.K., A Trustworthy System for Secure Access to Patient Centric Sensitive Information, *Telematics and Informatics* (2017), doi: https://doi.org/10.1016/j.tele.2017.09.008

A Trustworthy System for Secure Access to Patient Centric Sensitive Information

Navroop Kaur*, Yachana and Sandeep K. Sood

Guru Nanak Dev University Regional Campus Gurdaspur, India

Abstract

Smart technological innovations in healthcare are continuously generating digitized medical information about each patient, leading to the creation of Patient Centric Big Medical Data (PCBMD). Rapid adoption of PCBMD in healthcare ushers at the cost of its security and privacy concerns. Current methods focus on identifying authorized users who can access PCBMD but they barely identify the insider attackers. Alternatively, these methods do not prevent information leak by authorized users. Working towards this direction, this paper proposes a Trust based Access Control (TAC) system which not only identifies authorized users for PCBMD but also defends Sensitive Personal Information (SPI) of a patient from insider attacks. The proposed method calculates the trust value of each user by considering various quantitative parameters. Based on the calculated trust values, access rights are granted to each user such that SPI can be accessed by only highly trustworthy users. To implement access rights securely, a privacy scheme is also proposed. The experimental results show that the proposed security system can be efficiently used to protect the SPI of patients.

Keywords: Patient Centric Big Medical Data; Information Security; Privacy; Trust; Access Control.

1. Introduction

A colossal data set of digitized and accurate medical data of patients, persistently generated by the technological enhancements and smart innovations in medical field, is referred as Patient Centric Big Medical Data (PCBMD). Many useful predictions and information can be drawn from PCBMD with the application of effective mining techniques. For example, a doctor can get information about the medical condition of a patient and recommend better medications by comparing it with the other similar types of patients around the world. Similarly, an insurance company can devise more effective policies based on the available data. Although mining PCBMD leads to useful results, however, it paves its way to various security and privacy loopholes. For example, disclosure of sensitive patient's health data can result in its illegal use, thereby, putting millions of patient records at risk. Therefore, security and privacy of PCBMD is one of the major challenges in medical data mining.

The existing methods [1], [2] identify the authorized users who are allowed to have full access of data in PCBMD. Nevertheless, such systems fail to identify the insider attackers, leading to a problem of information leak by authorized users. Working towards this direction, the proposed system initially divides the information in PCBMD into two granular levels, namely, Sensitive Personal Information (SPI) and Non-Sensitive Personal Information (NSPI). SPI corresponds to that data which can potentially identify a particular individual. Alternatively, it is the information which, when disclosed, can result in privacy breach to the user. SPI includes: person's name, address, all elements of dates directly related to patient (e.g. D.O.B, admission date, discharge date, date of death), medical record number, medical conditions, health plan number, biometric identifiers (e.g. finger and voice prints), unique identifiers such as passport or SSN, personally identifiable financial information, photographs