Chapter 54
Medical Data Security Tools and Techniques in E-Health Applications

Anukul Pandey
Dumka Engineering College, India

Butta Singh
https://orcid.org/0000-0002-0170-6270
Guru Nanak Dev University, India

Barjinder Singh Saini
Dr. B. R. Ambedkar National Institute of Technology, India

Neetu Sood
Dr. B. R. Ambedkar National Institute of Technology, India

ABSTRACT

The primary objective of this chapter is to analyze the existing tools and techniques for medical data security. Typically, medical data includes either medical signals such as electrocardiogram, electroencephalogram, electromyography, or medical imaging like digital imaging and communications in medicine, joint photographic experts group format. The medical data are sensitive, subject to privacy preservation, and data access rights. Security in e-health field is an integrated concept which includes robust combination of confidentiality, integrity, and availability of medical data. Confidentiality ensures the data is inaccessible to unauthorized access. Integrity restricts the alteration in data by the unauthorized user. Whereas availability provides the readiness of the data when needed by the authorized user. Additionally, confidentiality, integrity and availability, accountability parameter records the back action list which answers the why, when, what, and whom data is accessed. The selected tools and techniques used in medical data security in e-health applications is discussed.

DOI: 10.4018/978-1-7998-8954-0.ch054

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

With the progressions in information and communication technologies (ICT) has unlocked fresher prospects for telemedicine(Ingenerf, 1999; Pattichis et al., 2002) by enabling medical data accessibility across geographical boundaries through Internet, mobile links, and other wireless/wired communication channels and thus covering rural/remote areas, accident sites, ambulance, and hospitals for e-health applications(Silva, Rodrigues, Canelo, Lopes, & Lloret, 2014). The histrionic expansion of contemporary communication technologies, the security of medical information has become an essential topic when it is transferred or deposited over open channels(Society, 1996).

Medical Data Security

Medical data attributes to the health-pertained information in association with the clinical trial program either in form of reports/signal/image(Hossain & Chellappan, 2014; Lu, Wu, Liu, Chen, & Guo, 2013; Yachana, Kaur, & Sood, 2017). Medical data also referred to as personal health information, commonly refers to geographic information, medical antiquities, assessment and laboratory results, mental/physical health situations, insurance information, and other data that a healthcare specialized gathers to classify an individual and govern suitable care. Medical data security is needed in e-health management framework due to essentially i) Medical data is having the capacity to reveal identity information, ii) prevent medical data tempering, which may mislead clinical diagnosis(A. Pandey, Saini, Singh, & Sood, 2017; Anukul Pandey, Saini, Singh, & Sood, 2018; Anukul Pandey, Singh, Saini, & Sood, 2016).

A patient privacy protection scheme for medical information system (Lu et al., 2013) is explored for the construction of the index of privacy data, and translation into a new query over the corresponding index for a query operation over privacy data so that it can be performed at the server side instantly. Prior to database storage at the server side of a medical information system, patient's privacy data being first encrypted to prevent the leakage of patient's private information caused internal staff. Based on millions of tuples of privacy fields experimental evaluation validate the effectiveness of patient privacy protection scheme.

MEDICAL DATA SECURITY TOOLS

FireHost

Texas-based FireHost is a cloud based Compliance as a Service (CaaS). The FireHost supplies CaaS with safeguarding the secret data and guaranteeing the necessities as documented in HIPAA. The multiple security yields are reduced by the FireHost (Chris Paoli, 2014).

FireLayers

FireLayers prevent unauthorized access with its new security access application for apps running in the cloud that offers surplus protection and monitoring. The FireLayers app security includes a dominant console with administrators control over guidelines, authorizations and admittance. FireLayers demonstrations recognized threats and employ rules to kiosk them and reports the precise limitations (Chris Paoli, 2014).

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/medical-data-security-tools-and-techniques-in-e-health-applications/280222

Related Content

Privacy and Security in the Age of Electronic Customer Relationship Management
Nicholas C. Romano Jr.and Jerry Fjermestad (2007). *International Journal of Information Security and Privacy (pp. 65-86).*
www.irma-international.org/article/privacy-security-age-electronic-customer/2457

An Adaptive Trustworthiness Modelling Approach for Ubiquitous Software Systems
Amr Ali-Eldin, Jan Van Den Bergand Semir Daskapan (2014). *International Journal of Information Security and Privacy (pp. 44-61).*
www.irma-international.org/article/an-adaptive-trustworthiness-modelling-approach-for-ubiquitous-software-systems/140672

A Literature Review on Image Encryption Techniques
S Geetha, P Punithavathi, A Magnus Infanteenaand S Siva Sivatha Sindhu (2018). *International Journal of Information Security and Privacy (pp. 42-83).*
www.irma-international.org/article/a-literature-review-on-image-encryption-techniques/208126

A "One-Pass" Methodology for Sensitive Data Disk Wipes
Doug Whiteand Alan Rea (2009). *Handbook of Research on Information Security and Assurance (pp. 193-201).*
www.irma-international.org/chapter/one-pass-methodology-sensitive-data/20650

Technical Report: A Visit on Coca-Cola Happiness Factory in Greater Noida
Neel Raiand Shivani Agarwal (2019). *International Journal of Risk and Contingency Management (pp. 74-78).*
www.irma-international.org/article/technical-report/216870