Chapter 7
Multi-Keyword Searchable Encryption for E-Health System With Multiple Data Writers and Readers

Dhruti P. Sharma
Sarvajanik College of Engineering and Technology, India

Devesh C. Jinwala
https://orcid.org/0000-0003-4830-1702
S. V. National Institute of Technology, India

ABSTRACT

E-health is a cloud-based system to store and share medical data with the stakeholders. From a security perspective, the stored data are in encrypted form that could further be searched by the stakeholders through searchable encryption (SE). Practically, an e-health system with support of multiple stakeholders (that may work as either data owner [writer] or user [reader]) along with the provision of multi-keyword search is desirable. However, the existing SE schemes either support multi-keyword search in multi-reader setting or offer multi-writer, multi-reader mechanism along with single-keyword search only. This chapter proposes a multi-keyword SE for an e-health system in multi-writer multi-reader setting. With this scheme, any registered writer could share data with any registered reader with optimal storage-computational overhead on writer. The proposed scheme offers conjunctive search with optimal search complexity at server. It also ensures security to medical records and privacy of keywords. The theoretical and empirical analysis demonstrates the effectiveness of the proposed work.

DOI: 10.4018/978-1-7998-6988-7.ch007

Copyright © 2022, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Since the last decade, several countries are moving towards digitization of medical records to improve data availability, data accessibility, data interoperability and data exchange (Akinyele et al., 2011; Löhr et al., 2010). Such digitized medical data would be effectively used in several applications concerning maintenance of health records in terms of EHR (electronic health record)(Rau et al., 2010; Schabetsberger et al., 2006), accounting and billing (Macdonald, 1986), medical research (Sunyaev et al., 2009). In practice, to offer ubiquitous access of data in cost effective manner, the exiting E-Health systems store medical data onto third party cloud server. Since such storage outsourcing may introduce risks of data leakage and security breach, most e-health systems offload encrypted data onto cloud server and subsequently use Searchable Encryption(SE) to search across the stored encrypted data. SE offers two significant features besides data privacy - (1) The data can be shared by the data owners (writers) to data readers and the reader has capability to query the shared data, (2) Query keywords and search operation would be secured in such a way that the service provider will be unable to access the unauthorized medical data stored over it(R. Zhang et al., 2017). There exist several different types of searchable encryptions based on - the cryptographic key(s) used for construction of ciphertext and search token, the structure of the search index used to compute ciphertexts, the number of keywords used to query data, the number of data writers and readers existed in system. Different E-Health systems require different searchable encryption schemes. Considering the number of writers/readers, the authors identify 4 different types of E-Health systems and suggest their suitable SE schemes - (1) When the outsourced data is created and accessed by the same user, then a Symmetric Searchable Encryption (SSE) could be used. For example, a hospital wants to maintain staff payroll, then an authorized accountant could store data onto could server and then would be able to search data from any location, (2) When a single data writer shares data with a single data reader, then any Public Key Searchable Encryption (PKSE) (Baek et al., 2008a; Boneh et al., 2004; Boneh & Waters, 2007) can utilize. Example, a patient shares his medical history with a doctor, (3) When a single data writer shares data with multiple data readers, then any multi-user searchable encryption scheme (Bao et al., 2008; Huang et al., 2016; Y. H. Hwang & Lee, 2007a; Kiayias et al., 2016; Lai et al., 2013; Wang et al., 2016; Ye et al., 2016; Y. Zhang et al., 2016)could be used. For example, a hospital wants to share the information about doctors currently working in that hospital with all registered patients, (4) When multiple data writers want to share data with multiple data readers, then either writer-managed multi-user SE(Bao et al., 2008; Huang et al., 2016; Y. H. Hwang & Lee, 2007b; J. Li & Chen, 2013) or trusted authority based multi-user SE could be used (M.-S. Hwang et al., 2014; Jingzhang et al., 2018; Kiayias et al., 2016; J. Li & Chen, 2013; Lv et al., 2014; Wang et al., 2016; Xu et al., 2019; Ye et al., 2016; Y. Zhang et al., 2016). An example of such E-Health system will be discussed in the Section **Problem Definition**.

Additionally, the existing SE schemes either offer search for a single keyword (Baek et al., 2008b; Boneh et al., 2004) or for multiple keywords (Ballard et al., 2005; Boneh & Waters, 2007; Byun et al., 2006; Z. Chen et al., 2012; Ding et al., 2012; M.-S. Hwang et al., 2014; Y. H. Hwang & Lee, 2007a; B. Zhang & Zhang, 2011)based on number of keywords allowed in search query. In practice, an E-Health system offering multi-keyword search by the stakeholders(viz. hospitals, pharmacy, insurance company etc.) is more desirable.

23 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/multi-keyword-searchable-encryption-for-e-health-system-with-multiple-data-writers-and-readers/287167

Related Content

Survey and Evaluation of Advanced Mobility Management Schemes in the Host Identity Layer
László Bokor, Zoltán Faigland Sándor Imre (2014). *International Journal of Wireless Networks and Broadband Technologies (pp. 34-59).*
www.irma-international.org/article/survey-and-evaluation-of-advanced-mobility-management-schemes-in-the-host-identity-layer/104629

Link Failure Avoidance Mechanism (LFAM) and Route Availability Check Mechanism (RACM): For Secure and Efficient AODV Routing Protocol
Meeta Singhand Sudeep Kumar (2018). *International Journal of Wireless Networks and Broadband Technologies (pp. 1-14).*
www.irma-international.org/article/link-failure-avoidance-mechanism-lfam-and-route-availability-check-mechanism-racm/209431

Video Streaming Based Services over 4G Networks: Challenges and Solutions
Alvaro Suarez (2010). *Fourth-Generation Wireless Networks: Applications and Innovations (pp. 494-525).*
www.irma-international.org/chapter/video-streaming-based-services-over/40715

Energy Efficient Wireless Body Area Network (WBAN)
Prasenjit Maiti, Sourav Kanti Addya, Bibhudatta Sahooand Ashok Kumar Turuk (2017). *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures (pp. 413-432).*
www.irma-international.org/chapter/energy-efficient-wireless-body-area-network-wban/162129

Detection of Virtual Private Network Traffic Using Machine Learning
Shane Miller, Kevin Curranand Tom Lunney (2020). *International Journal of Wireless Networks and Broadband Technologies (pp. 60-80).*
www.irma-international.org/article/detection-of-virtual-private-network-traffic-using-machine-learning/257779