Chapter 10
A Conceptual Framework for an Extension Access Control Models in Saudi Arabia Healthcare Systems

Amin Shaqrah
Taibah University, Saudi Arabia

Talal Noor
Taibah University, Saudi Arabia

ABSTRACT

This article aims to develop an extension access control models framework in Saudi Arabian healthcare systems. The conceptual framework acts as an ascendency structure to organize and support the efforts of several health care standards which reflect on the coherent of confidentiality; integrity; and availability triads in order to achieve the strategic business objectives of Saudi Arabian healthcare institutions. It is considered to be three common access control models developed by ACM institute and extended to other criteria identified by the National Institute of Standards and Technology. While literature explains that an easy-to-use access control model can lead to success healthcare system, understanding the extension of access control systems is vital for Saudi Arabian healthcare institutions to protect resources against unauthorized use. This article has taken a step in this direction.

INTRODUCTION

The purpose of information security in Healthcare Information Systems (HIS), in general, is to guarantee the Confidentiality, Integrity, and Availability (CIA) of the data (Srisakthi and Shanthi, 2015). Confidentiality of the data is the protection that only those with appropriate rights and verified permissions might access certain data (Whitman et al., 2013). Data should not be disclosed to unauthorized entities, integrity in general means sustaining and ensuring the accurateness of data over its entire life cycle.

DOI: 10.4018/978-1-7998-1204-3.ch010

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

In HIS, integrity of the data means that data should not be modified by unauthorized entities/persons. Protection of data in HIS prevents unofficial or accidental with holding of data or resources. To insure HIS security, countries initiate laws and regulations that healthcare organizations must follow. In the US there are three acts, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leah Bliley Act (GLBA), and the Sarbanes Oxley Act (SOX), that involve statements to protect personal information from being revealed or retrieved by unofficial persons, entities, or processes (Gopalan et al., 2012). HIPAA upholds principles for the practice and release of Protected Health Information (PHI), which is any data about health status, provision of health care, or health care expenses that can be connected to an individual (Lerouge, et al., 2007).

To protect PHI, healthcare organizations need to enforce the patients' rights by using a set of policies and technologies. Access control models were introduced to overcome the privacy matter and grant permission to access PHI to only authorized persons. Access control models are used to prevent unofficial use of resources, including using resources in an authorized manner (Zeltsan, 2010). There are many access control models, each of these models have been extended in different ways to cover missing security measures. Healthcare organizations are free to choose the specific access control model that fits the organization's needs and is compatible with PHI privacy regulations. In addition to laws, regulations, policies and technology, standards are also used to confirm the security of the PHI in healthcare information systems (Fichman and Kemerer, 1997). Standards can be used to deliver the basic required measures to help enforcing and maintaining information security procedure in any institution. There are few well-known standardization tier-1 organizations such as the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Association of Computing Machinery (ACM). There are other standardization organizations specific to certain industries. For example, Health Level Seven (HL7) addresses concerns about healthcare informatics. The industry standardization organizations generally adopt the technology that has been used by tier-1 standardization entities (Meyer and Goes, 1998). The literature study did not provide a methodology to extend for achieving the NISTER, the presented paper provides a starting point to meet the need for developing an extension access control model framework that addresses the synergy between secure healthcare systems and access control models considering NISTER 7874. The rest of this paper is structured as follows: Saudi Arabia health care systems, an overview of access control model, assessment access control model, proposed framework, implication, finally the conclusion and future work.

SAUDI ARABIA HEALTH CARE SYSTEMS

The unsettled environment of the healthcare sector growing the importance to adopt new technologies to achieve the vision of healthcare institutions (Samarati et al., 2001, Rossetti et al., 2012 and Hoeur and Kritchanchai, 2015). This section will provide the current requirement for healthcare systems. As mentioned in the definition of the access control, its purpose is to prevent unauthorized access to PHI. Conell and Young (2007) assertion the general privacy needs from the ACM are: 1) Healthcare institutions requirements have the ability of having the choice of designing the security policy, and the resilience to randomly define the security of PHI. 2) Patient requirements to have the ability for having full control over their PHI, right to disclose certain information, and transfer the rights from one healthcare provider to another. 3) Ease of handling ACM. Recently, the office of the National Coordinator for Health Information Technology published guidelines to preserve privacy and security related to PHI (Canada

10 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/a-conceptual-framework-for-an-extension-access-control-models-in-saudi-arabia-healthcare-systems/243111

Related Content

Data Science Techniques in Knowledge-Intensive Business Processes: A Collection of Use Cases for Investment Banking
Matthias Ledererand Joanna Riedl (2020). *International Journal of Data Analytics (pp. 52-67).*
www.irma-international.org/article/data-science-techniques-in-knowledge-intensive-business-processes/244169

Loan Fraud Detection Using Machine Learning as a Data Mining Approach
Nabila Hamdoun (2022). *International Journal of Data Analytics (pp. 1-10).*
www.irma-international.org/article/loan-fraud-detection-using-machine-learning-as-a-data-mining-approach/309096

Focused Error Analysis: Examples from the Use of the SHEEP Model
Deborah J. Rosenorn-Lanngand Vaughan A. Michell (2016). *International Journal of Big Data and Analytics in Healthcare (pp. 30-48).*
www.irma-international.org/article/focused-error-analysis/171403

Development of Data Analytics in Shipping
Lokukaluge P. Pereraand Brage Mo (2017). *Privacy and Security Policies in Big Data (pp. 239-258).*
www.irma-international.org/chapter/development-of-data-analytics-in-shipping/179138

Use-Case Driven Approach for a Pragmatic Implementation of Interoperability in eHealth
Karima Bourquardand Alexander Berler (2020). *Data Analytics in Medicine: Concepts, Methodologies, Tools, and Applications (pp. 357-368).*
www.irma-international.org/chapter/use-case-driven-approach-for-a-pragmatic-implementation-of-interoperability-in-ehealth/243120