
Amin Shaqrah, College of Computer Science and Engineering in Yanbu, Taibah University, Medina, Saudi Arabia
Talal Noor, College of Computer Science and Engineering in Yanbu, Taibah University, Medina, 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.

KEYWORDS


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. 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 Health Infoway, 2015), the guidelines suggested that healthcare institutions have to address the following points: 1) auditing functions, 2) unique user IDs and strong passwords, 3) Role or User-based Access Control, 4) auto time-out, 5) amendments and accounting of disclosures (Cresswell and Sheikh, 2013). Currently, most of the healthcare systems are integrated using traditional technologies and standards (Almadani et al., 2016); security is the most important issue when integrating healthcare systems. The KSA healthcare system currently faces numerous challenges and the MOH is under remarkable pressure from its government to develop a high-quality healthcare system and improve healthcare services to all residents, mainly in rural/remote areas (Khudair, 2008). In 2010, the MOH conducted a study into the adoption of telemedicine stating that telemedicine abilities can improve many challenges of the KSA healthcare system (El-Mahalli et al., 2012). In 2011, the MOH launched the first national project for telemedicine, referred to as the Saudi Telemedicine Network (STN), covering all Healthcare Facilities (HCF) (MOH, 2016).

Alaboudi (2016) noted Saudi Arabia healthcare system exposed to various obstacles and even MOH pressures to offer high quality healthcare services to all residents, mostly in rural areas, ministry of health on (2010) initiate telemedicine adoption. Alkhamis and Hassan (2014) concluded the variances among literature with respect to adopt telemedicine. Alkhamis (2017) and Aljazaeri (2017) resolve the amount which MOH support healthcare systems. Saudi Arabian MOH deploy a complete package of health care management through the main solution to manage the “OASIS”
Constructing Temporal Equivalence Partitionings for Keyword Sets
www.igi-global.com/article/constructing-temporal-equivalence-partitionings-for-keyword-sets/129071?camid=4v1a

Four Express Service Cooperation Modes for B2C E-Commerce: Models and Analysis
www.igi-global.com/article/four-express-service-cooperation-modes-for-b2c-e-commerce/133148?camid=4v1a