Behavior-Based Access Control for Distributed Healthcare Environment

Mohammad H. Yarmand, Kamran Sartipi and Douglas G. Down
Dept. Computing and Software, McMaster University
Hamilton, ON, L8S 4K1, Canada
{*yarmanmh, sartipi, downd*}*@mcmaster.ca*

Abstract

Sensitivity of clinical data and strict rules regarding data sharing have caused privacy and security to be critical requirements for using patient profiles in distributed healthcare environments. The amalgamation of new information technology with traditional healthcare workflows for sharing patient profiles has made the whole system vulnerable to security and privacy breach. In this paper we present a novel access control model based on a framework designed for data and service interoperability in the healthcare domain. The proposed model for customizable access control captures the dynamic behavior of the user and determines access rights accordingly. The model is generic and flexible in the sense that an access control engine dynamically receives security effective factors from the subject user, and identifies the privilege level in accessing clinical data using different specialized components within the engine. Standard data representation formats are used to make the model compatible with different healthcare environments. The access control engine uses a flow-based approach to follow the user's behavior and navigates between engine components to provide a final weighted value representing the privilege to access a resource. The proposed model is supported by a real world case study.

KEYWORDS: Security; Context Aware Access Control; Healthcare; Behavior; HL7; Patient Data.