Ongoing Research in Biomedical Informatics on Access Control and Cloud Computing using FHIR

The healthcare domain can be seen as an emergent application for cloud computing, in which the Meaningful Use Stage 3 guidelines recommend any health information technology (HIT) system to provide cloud services that enable health-related data owners to access, modify, and exchange such data. This requires mobile and desktop applications for patients and medical providers to obtain health information from multiple HITs, that may be operating with different paradigms (e.g., cloud services, programming services, web services), use different cloud service providers, and employ different security/access control techniques. Health Information Exchange (HIE) provides a more complete health record of an individual that improves patient care with relevant data gathered from multiple health information technology (HIT) systems. In support of HIE, the Health Level Seven (HL7) XML standard was developed to manage, exchange, integrate, and retrieve electronic health information. In 2011, HL7 began drafting a next-generation standard, Fast Healthcare Interoperable Resources (FHIR), to facilitate the development and interaction of mobile health (mHealth) apps, HIT data sharing, and common format for information modeling. FHIR is based on RESTful APIs and supported by a FHIR server infrastructure that facilitates the exchange in a cloud computing setting. FHIR while possessing a security specification, has yet to define and identify actual security mechanisms for secure data exchange via RESTful API calls. The need to develop mobile applications and services has dramatically increased in the marketplace, with the Gartner group forecasting the business demand for new and diverse mobile applications by the end of 2017 will grow five times larger than the ability of a typical IT organization to deliver. The HL7 Fast Healthcare Interoperability Resources (FHIR) standard is designed to enable interoperability and integration with the newest and adopted technologies by the industry. This is facilitated via a FHIR server that provides a RESTful CRUD services to access an HIT system. In support of this broad area, we are conducting work with complementary foci:

- **A Mobile Health Application for Medication Reconciliation**: This work is currently underway (Agresta, Demurjran, Sanzi) [II] which and involves Medication Reconciliation which is one of the most critical aspects of patient care that needs to be achieved at the earliest stages of the diagnostic process which is hampered by the fact that a patient’s medications might be located in multiple HIT systems such as electronic health records (EHRs) (at physician offices, hospitals, clinics, etc.) and pharmacy systems. The intent of the proposed work is to provide a mechanism that will offer patients in medical providers a Best Possible Medication History (BPMH). Our expectation of participating in ABCT is to transition the proof of concept prototype that was developed in the recent contract towards a alpha/beta product through process of user Center design via stakeholders that include patients, medical providers, home health practitioners, visiting nurses, etc. The intent is to develop both a mobile health application that has a back and server with the programmatic algorithm able to take medications for a given patient from multiple sources and before medication reconciliation in order to return a Best Possible Medication History (BPMH). The server portion of medication reconciliation and it’s associated algorithm will be invertible into electronic health record products using the Smart on FHIR framework (https://docs.smarthealthit.org/).

- **Lattice-Based Access Control (LBAC) to Control Healthcare Data**: This work is currently underway (Demurjran, Agresta) [I] utilizes our prior work [V] on multi-level security for healthcare that we developed and explore alternative approaches to integrate this approach into Fast Healthcare Interoperability Resources (FHIR). FHIR provides structures for sharing EHR data between healthcare providers. Data is accessed through resources utilizing a location URL as part of a REST API in conjunction with a logical ID. This allows data that resources describe to sync between separate FHIR systems. We focus on the FHIR base resources (e.g., patients, practitioners, and family relationships; organizations, services, appointments, and encounters) and clinical resources which are for a patient’s health history. Note that these alternative approaches are described at the specification level of the FHIR resources and not from an implementation perspective.

- **Role-Based Access Control (RBAC) for Mobile Computing**: Our initial work in this area (Rivera Sanchez and Demurjran 2016) focused on user authorization requirements for mobile computing that then led work on the incorporation of API-based role-based access control (RBAC) (Rivera Sanchez, et al., 2016) in a mobile application and its server/database. In (Rivera Sanchez, et al., 2017), we incorporate role-based access control (RBAC) into FHIR to support the ability to control access of who can call which services of FHIR RESTful APIs that manage sensitive healthcare data. The work was demonstrated utilizing a mHealth application that communicates with the OpenEMR electronic health record via the HAPI FHIR server.

- **Blueprints of Architectural Design for Integrating mHealth Apps with HITs via FHIR**: This work (Baihan, et al., 2017) presents a number of blueprints for the design and development of FHIR servers that enable the integration between HIT systems with mHealth applications via FHIR. Each blueprint is based on the location that FHIR servers can be placed with respect to the components of the mHealth application (UI, API, Server) or a HIT system in order to define and design the necessary infrastructure to facilitate the exchange of information via FHIR. To demonstrate the feasibility of the work, this chapter utilizes the Connecticut Concussion Tracker (CT²) mHealth application as a proof-
of-concept prototype that fully illustrates the blueprints of the design and development steps that are involved. The blueprints can be applied to any mHealth application and are informative and instructional for medical stakeholders, researchers, and developers.

- **Framework for Secure and Interoperable Cloud Computing:** The effort reported in (Baihan and Demurjian, 2017) supports a global security policy and enforcement mechanism access to cloud services with role-based, discretionary, and mandatory access controls. To support interoperability and exchange of healthcare data, the Health Level 7 (HL7) standards organization has proposed the Fast Healthcare Interoperability Resources (FHIR) which models healthcare data with XML or JSON schemas in a set of 93 resources to track a patient’s clinical findings, problems, allergies, adverse events, history, suggested physician orders, care planning, etc. For each resource, a FHIR CRUD RESTful Application Program Interface (API) is defined to share data in a common format for each of the HITs that can then be easily accessible by mobile applications. In such a context, there is a need to support with a heterogeneous set of information sources and differing security protocols (such as role-based, mandatory, and discretion access control). To demonstrate the realization of FSICC, the framework has been applied to the integration of the Connecticut Concussion Tracker (CT2) mHealth application with the OpenEMR electronic medical record utilizing FHIR.

- **Adaptive Trust Negotiation for Time-Critical Access to Healthcare Data:** Adaptive trust negotiation (Sanzi et al., 2016) in a mobile environment is a means to dynamically adjust security parameters based on the level of trust established during the negotiation process thereby enhancing mobile security via a trust profile that contains a proof of history of successful access to sensitive data to facilitate identification and authentication that requests data from a server where no relationship between the user and server has previously existed as a result of trust negotiation. Using that as a basis, our recent work (Sanzi and Demurjian 2017) proposed a new model of trust negotiation using role-based and attribute-based access control that defines a new trust profile that contains a collection of credentials describing the user’s access history. As a result of our work, an authorization system based on trust negotiation can examine the user’s history in detail, decide whether to authorize the user, and add its own record of user access to the user’s trust profile that can be utilized in future attempts at access at other locations. As a proof of concept, our work has been integrated into the Connecticut Concussion Tracker (CT2) mobile application and server.

- **Spatio-Situation-Based Access Control Model for Dynamic Permissions:** Medical providers often give care in multiple locations in a given day. For example, a physician using a mHealth app to access patient data may move from his office EHR to a hospital EHR across the street to a clinic’s EHR in a neighboring town etc. When the physician moves to a location far enough away for differentiation via GPS, a dynamic adjustment by time and space (spatio) could be utilized to prohibit access to the office EHR while allowing access to the hospital EHR. To address these and other issues our effort (Shao et al. 2016) presented a Spatio-Situation-Based Access Control (SSBAC) model that extends RBAC to secure sensitive data for mobile applications with the ability to make dynamic authorization decisions according to the time/location and the particular situation being encountered by a user. The SSBAC model allows authorizations to be defined based on a combination of: the actual time that a user is utilizing a mobile application, the physical location of the user, and/or the activities that a user is performing (situation). As a result, the mobile application can dynamically adjust in terms of the information that is accessible/prohibited.

- **Large-Scale Architectural Alternatives for HIE:** In this work, the problem involves adoption of health information systems and the integration of healthcare data and systems into efficient cross-institutional collaboration workflows of stakeholders (e.g., medical providers such as physicians, hospitals, clinics, labs, etc.) which is a challenging problem for the healthcare domain. Our first work in this effort (Ziminski et al., 2015) studied the way that well-established software engineering architectural styles can be employed to satisfy requirements of the healthcare domain and ease health information exchange (HIE) between stakeholders. Towards this goal, work proposed a hybrid HIE architecture (HHIEA) that leverages the studied styles that include service-oriented architecture, grid computing, publish/subscribe paradigm, and data warehousing to allow the health information systems of stakeholders to be integrated to facilitate collaboration among medical providers. To demonstrate the feasibility and utility of HHIEA, a realistic regional healthcare scenario in introduced that illustrates the interactions of stakeholders across an integrated collection of health information system. Ongoing work is extending the work to include the assessment and utilization of FHIR.
Related to healthcare since 2009, S. Demurjian and T. Agresta have 17 publications (I to XVII) with other colleagues and undergraduate and graduate students and S. Demurjian as an additional 33 publications (XVIII to L) with other colleagues, undergraduates and graduate students. Publications that are relevant to this proposed ABCT in medication reconciliation are [II, XLIII], healthcare interoperability architectures [III, VI, XIV, XII] lattice-based access control for fine grained access to healthcare data [I, V], adaptive trust that negotiation for mobile health applications [X, XVIII, XXVIII, XXVIII, XXX] access control for mobile health applications [IV, IX, X, XXVIII, XXVI, XXVIII, XXX], access control for cloud computing applications usable data [I, V], adaptive trust that negotiation for mobile health applications [X, XVIII, XXVIII, XXX] access control for healthcare standards such as HL7 [XXIX, XXXVII, XXVIII, XL, XLI, XLIII], semantics and ontology design and development for healthcare [XIII, XXV, XXXIII, XXXVII, XXVIII, XLIV, XLVII], and collaborative security for healthcare [XVI, XVII, XXXII, XXXIV, XLVIII].

Publications Related to the Healthcare Domain with T. Agresta


Other Healthcare Publications of S. Demurjian


Biomedical Informatics at UConn Storrs and UCHC Farmington

Profs. Steven A. Demurjian and Thomas Agresta
steven.demurjian@uconn.edu and agresta@uchc.edu

Current Ph.D. Students: David Etim, Zion Emmanuel and Timo Ziminski

Recently Completed Ph.D. Students: Yaira K. Rivera-Sanchez, Eugene Sanzi, Mohammed Baihain, Alberto De La Rosa Algarin, and Rishi Sariapalle Knath


Other Biomedical Publications:


