An Activity Theory Approach to Specification of Access Control Policies in Transitive Health Workflows

Research-in-progress

Rohit Valecha
University at Buffalo
Buffalo, New York, USA
valecha@buffalo.edu

Mandvika Kashyap
University at Buffalo
Buffalo, New York, USA
mandvika@buffalo.edu

Swathi Rajeev
University at Buffalo
Buffalo, New York, USA
swathira@buffalo.edu

H. Raghav Rao
University at Buffalo
Buffalo, New York, USA
mgmtrao@buffalo.edu

Shambhu Upadhyaya
University at Buffalo
Buffalo, New York, USA
shambhu@buffalo.edu

Abstract

Access control models are implemented to mitigate the risks of unauthorized access in Electronic Health Records (EHRs). These models provide authorization with the help of security policies, wherein the protected resource is governed by one or more policies that exactly specify what attributes a requester needs to fulfill in order to obtain access. However, due to the increasing complexity of current healthcare system, defining and implementing policies are becoming more and more difficult. In this research-in-progress paper, we present an Activity Theory driven methodology to formalize access control policies that can be used in enforcing patient's privacy consent in a healthcare setting. In order to account for the transitivity in health workflows, we extend the Activity Theory to include "organizational interconnectedness" within the health workflows.

Keywords

Activity Theory, Organizational Interconnectedness, Electronic Healthcare Records, Transitive Health Workflows, Access Control Policy, Policy Specification, Policy Formalization, XACML Policies

Introduction

Governments and institutions have started to recognize the importance of the exchange of Electronic Health Records (EHRs) between hospitals. This exchange process is regulated by the patients, who decide who has the rights to access their personal healthcare data and who has not. In order to mitigate the risks of unauthorized access in Electronic Health Records (EHRs), access control models are implemented to safeguard patient's privacy consent. One such type of model that requires establishing security policies to ensure users can only access what they are authorized to (Busch et al., 2012) is Policy Based Access Control (PBAC) model, wherein a protected resource is governed by one or more policies that specify what attributes a requester needs to fulfill in order to obtain access (Margheri et al., 2013a).

However, defining and implementing access control policies has become increasingly difficult (Margheri et al., 2013b) owing to the complexities of the healthcare systems: 1) patient workflows are growing transitive in nature, as the data flows from one point to the other in the workflow (Valecha et al., 2012); 2) privacy consent is becoming intricate due to the regulations by multiple legislations that vary from region to region; 3) technology to meet patient's needs is fragmented. As a solution to this problem, we provide a theory-driven methodology to enable the formalization of access control policies.

The healthcare workflow consists of complex activities typically involving multiple agencies. Shanker et al. (2009) suggest that Activity Theory can be used to simplify the complex workflows. Activity Theory is a powerful and clarifying descriptive tool with the objective to understand the activity (Nardi, 1995). It gives the flexibility of breaking up complex tasks into activities that are easy to interpret and manage. Consequently, we use Activity Theory as a lens to deconstruct the complex activities in the health workflow, and then develop our framework to enforce patient's privacy consent in a complex healthcare setting with an aim to address the research question: how to clearly define and implement access control policies in a transitive healthcare workflow?

Our contributions are two-fold: First, we extend Activity Theory to include "organizational interconnectedness" in a transitive health workflow. Second, we present a novel methodology to formalize the access control policies based on the extended Activity Theory. We specify the authorized policies in eXtensible Access Control Modeling Language (XACML) since it is the de-facto standard used in EHRs systems (De la Rosa Algarin et al., 2012). Our paper adheres to the design science research guidelines proposed by Hevner et al. (2004) and others (Peffers et al. 2003; Purao et al. 2008): the research contributes to the policy-based access control literature using an Activity Theory approach.

In the remainder of this paper, we first examine the existing literature on healthcare access control and Activity Theory. We then present the policy specification design consideration followed by the new policy specification methodology. Finally, we discuss the paper's implications and limitations, and suggest directions for future research.

Background

In this section, we discuss some of the current access control models including access control lists, role-based access control, attribute-based access control and policy-based access control. Subsequently we introduce Activity Theory and discuss its potential in helping us elicit and understand the requirements in the policy specification process.

Access Control

Access Control Lists (ACLs) are the oldest and the simplest form of access control wherein each resource on a system has its own list of mappings between the set of requesting entities and their set of actions (Nita-Rotaru & Li, 2004). ACLs are difficult to manage in an enterprise setting, in which the user has different levels of access to different resources, since adding, deleting and updating ACLs can be time-consuming and error-prone (Ferraiolo et al., 2003). Role-based Access Control (RBAC) is an alternative access control model in which access to a resource is determined based on the role of the requester (Sandhu et al., 1996). One of the disadvantages of RBAC is that dividing people into role categories makes defining granular access controls for each person cumbersome (Azhar et al., 2012). The Attribute-based Access Control (ABAC) model was designed to fulfill this requirement.

ABAC is an access control model wherein the access control decisions are made based on a set of attributes, associated with the requester, the environment, and the resource itself (Goyal et al., 2006). One limitation of the ABAC model is that in an enterprise setting with many resources, individuals, and applications, there can be disparate attributes and access control mechanisms (Reddivari et al., 2005). Policy-based Access Control (PBAC) enables organizations to have a more uniform access control model throughout the organization. Many organizations are discovering that they need to create and enforce policies that define who should have access to what resources, and in what environment. The eXtensible Access Control Markup Language (XACML) was developed as a way to specify access control policy in a machine-readable format (Anderson et al., 2003).

XACML-based Access Control

Access control is the process of mediating request to data, and determining if the request should be granted or denied. A typical access control model includes three main entities – subject, resource and action – a subject requests an action on a resource. In the healthcare setting, access control is the process of authorization in which the access to medical records can be limited only to users with an appropriate role and the access can be allowed only during an episode of care (Milutinovic, 2008).

Extensible Access Control Markup Language (XACML) (Anderson et al., 2003) is a standard that describes a policy in terms of request/response (written in XML). It defines an access control policy by providing features to express policy rules for resources in XML (Busch et al., 2012). The typical setup involves a subject requesting an action on a resource in the form of request for that resource. This request also includes the environment within which the action is to be performed. All the elements of the request have their own attributes, which are named values of known types. Specifically, attributes are characteristics of the subject, resource, action or environment in which the access request is made (Sanchez et al., 2008). For example, a user's name, their security clearance, the file they want to access, and the time of the day are attribute values for subject, action, resource and environment respectively. This request forms a query that is evaluated to determine whether the action should be allowed. The response is an expression about whether the request should be permitted or denied.

In order to derive these attributes within a healthcare setting, it is important to first deconstruct the transitive health workflows. Activity Theory can be used to simplify the complex workflows (Shanker et al., 2009). We discuss the use of Activity Theory in formalizing the access control policies next.

Activity Theory

Activity Theory is a framework that provides a lens to analyze the activity of a group or an organization (Chaudhury et al., 2001). It considers an activity consisting of six major elements: subject, object and community supported by tools, rules and division of labor. It suggests that an activity is directed towards an object, mediated by the instrument and socially constituted within the environment (Bertelsen and Bodker, 2003). The subject is the individual or the group performing the activity supported by instruments on the object that can be either an ideal or a material object (Valecha et al., 2012). This interaction between the subject and object is confined within the environment consisting of rules, responsibilities and communities (Chen et al., 2013). Engestrom (1999) extends the concept of Activity Theory, and gives a specific example of its usage in a hospital setting where a doctor performs a diagnosis on a patient. In this diagnosis activity, the subject is the physician, the object is the patient, and the activity is supported by the instruments such as stethoscope. The community in which the activity is placed is the physician and nurse, with constraints of patient authorization before disclosure to any entity, and responsibility of assisting the patient.

The healthcare system is a complex system that involves transitive workflows, intricate legislations and ever-expanding technology. The principal components (e.g., subject) of the healthcare workflow change depending on the circumstances, and their relationships within the environment undergo frequent restructuration. We apply Activity Theory to investigate healthcare systems along dimensions of an activity system: subject, activity, instrument, community, rule, and division of labor. This allows us to obtain an in-depth understanding of the healthcare setting, which allows us to comprehend the business requirements of access control policy and to recognize the key data elements that policy designers will value and will communicate during the data flow. In our study, we capture all of these key data elements and their interactions in our policy.

To formalize access control policies in a healthcare setting, we need to consider the transitivity within its workflows. Consequently, we extend Activity Theory. We start with the traditional formalisms of Activity Theory (Engestrom 1987), and then consider "organizational interconnectedness" as an important perspective. Our analyses of organizational interconnectedness between activity systems allow us to observe the data flow from one organization to the other, and to capture important data elements. Boer et al. (2002) studied "temporal interconnectedness" among multiple heterogeneous activity systems and Chen et al. (2013) investigated "temporal interconnectedness" within the activity system. While these studies consider transition from one activity system to another over a time sequence, we consider this transition over an organization sequence. The organization sequence reveals the pattern of information flow in the health workflow.

We argue that this organization sequence is inherent to the healthcare activities and affects the major constructs in Activity Theory. In health workflow system, there are different roles within the organization that do not cross the organizational boundaries. For example, an administrative role in a hospital provides read/write permission to patient's health condition, while an administrative role in an insurance agency provides read/write permission to patient's claims data. This results in role conflicts between the organizations. The organizational interconnectedness provides a higher level of abstraction that allows us to address conflicts that arise because of boundary transitions.

We also suggest that "feedback" in the form of request/response may exist between the organizations in a transitive workflow. Feedback is an implied part of Activity Theory (Foorthuis et al. 2008) that might exist among heterogeneous activity systems (Zhang and Bai 2005). Based on the existing literature, we recognize the potential effects of feedback in driving the development of our multi-organization activity system. The concepts of organizational interconnectedness and feedback are illustrated in Figure 1.

The data in a transitive health workflow passes between four types of organizations: providers, payers, purchasers and members. The Provider activity system consists of physicians, nurses, hospitals, and others that provide medical services. The Payer activity system includes employers, federal government, insurance companies, health plans, or other entities that is liable for healthcare coverage for plan members. The Purchaser activity system involves persons or organizations that actually pay the premiums for the healthcare plan. The Member activity system considers enrolled population of individuals for which a health plan provides a range of healthcare services. While the components (e.g., subjects, objects, rules) of the activity system sharply differ, they share portions of task-critical data (e.g., community, tool, responsibility) that can be incorporated into access control policies. We used XACML to specify and record the access control model. Where the organizations are concerned, XACML-based specification allows the platform-interdependent utilization of the development of automated authorization tools.

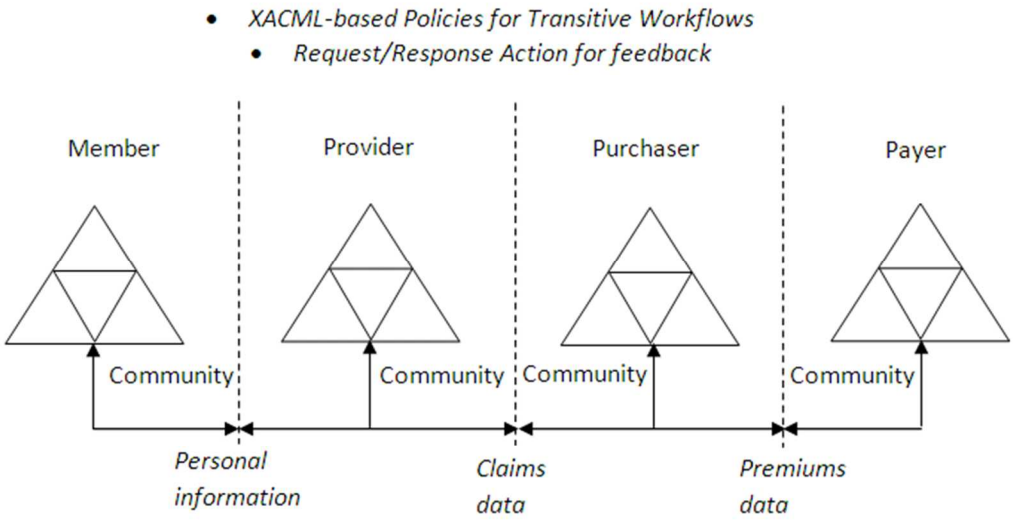

Figure 1. Organizational Interconnectedness in Health Workflow

Design Consideration for Policy Specification

In order to use Activity Theory to specify policy, first it is important to understand the elements of the policy and how they interact with each other. Thus in this section we detail the access control policies and access requests.

The basic element of the policy is <Policy>. A <Policy> is composed of a <Target>, which identifies the set of attributes that the requester must expose, <Obligation>, which determines the set of actions the user is obligated to perform, and <Rule>, which specifies the logic for access control decision by means of an

Effect, which can be either Permit or Deny. These elements are described in Table 1 below. A <Rule> may specify a <Target> and a <Condition> of its own, a combination of standard-defined functions that operate on values coming from the request (Busch et al., 2012).

A policy specifies of four elements within its target: <Subjects>, <Actions>, <Resources>, and <Environments>, each of which contains an attribute identifier, a value and a matching function. Together this information is used to check whether the policy is applicable to a given request. For example, a physician trying to request a read access to a resource with a code identifier 34133-9 for a healthcare TREATMENT. The matching function retrieves a value from the request and matches it with the values specified in the target element, according to the function's semantics. If, for all four categories, the matching of a target element succeeds, then the policy is applicable to the request (Margheri et al., 2013b). This is summarized in Figure 2 below.

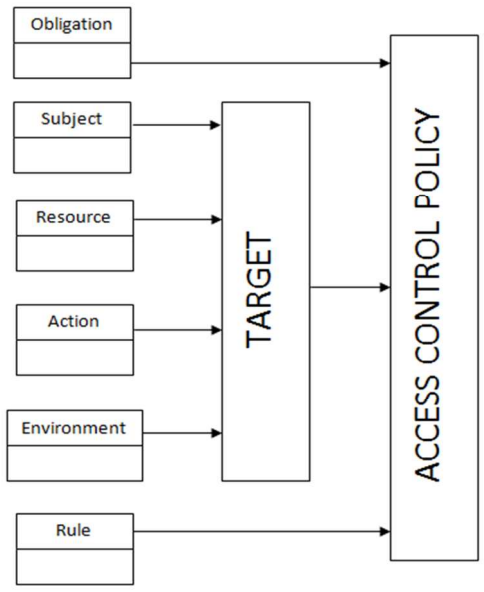

Figure 2. Policy Model

Table 1. Policy Elements

Entity	Description
Access Control Policy	
Obligation	A set of actions that is bound for the request
Rule	A set of conditions that the request has to satisfy
Target	A set of attributes (subject, resource, action, environment) that the request has to consist
Access Control Target	
Subject	The user requesting the access to the resource
Resource	The entity (patient data) being protected
Action	The operation to be performed on the resource
Environment	The setting in which the resource resides

Activity Theory Based Policy Specification

In this section, we elicit our Activity Theory approach to specify access control policy specification. An access control policy is composed of components in security systems and interactions among them (Huang & Kirchner, 2011). So the next step is to identify which aspects of an Activity Theory based analysis can help us to capture a view of access control policy that should be incorporated in the patient's privacy consent. This access control policy should include the acting subjects, the objects towards which activities are directed and the community as well as the mediating components, like rules or tools.

In an access control model, subject performs the activity of requesting access. The resource transformed by the access is a data or service. The obligation is the operation that is performed for enforcement of the authorization. The environment component is intended to specify aspects of the external environment and other additional information. The rules specify the logic for the access control decision by means of an effect. The action defines the type of access requested on the object. Thus, we propose a mapping from the basic structure of an activity into policy model of access control as depicted in Figure 3.

It is important to point out that we do not think that a strict, one to one mapping exists. Our view on access control policy is that different interpretations exist. For example, that what is considered

environmental information in one setting can be part of the rule in another setting. Likewise, the same piece of information can be part of different categories based on the task. The same holds for the Activity Theory based analysis itself: the same thing can be an object and a tool in different task settings. The mapping from activity system to policy system suggests that Activity Theory should lead the policy specification process and allow the designer to focus on task-related information instead of being lost in the modeling of policy details without being able to see the relationship between different aspects of the policy system (Kofod-Petersen & Cassens, 2006).

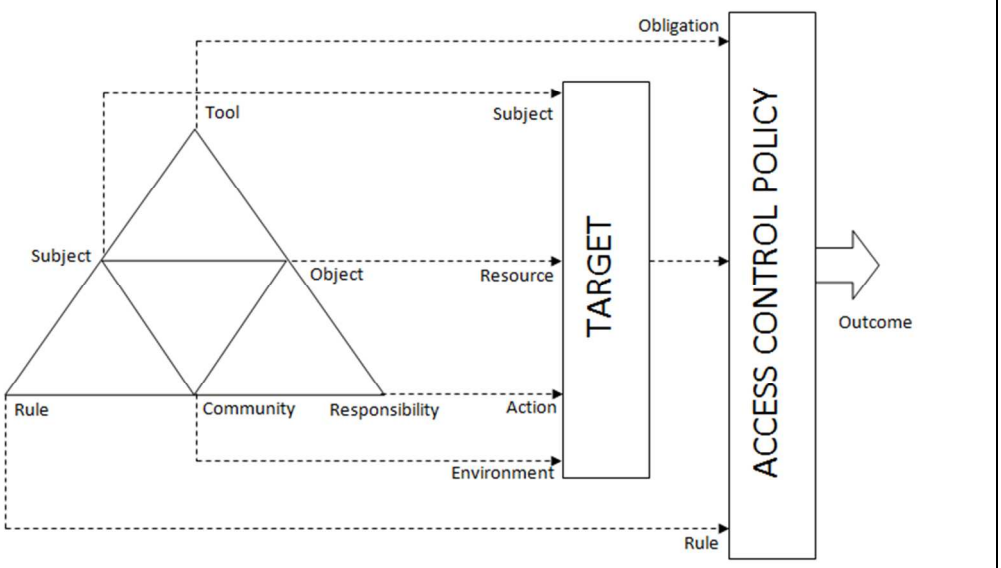

Figure 3. Activity Theory based Specification of Access Control Policy

Case Study

Let us now consider a hospital setting where a physician is requesting a read access to patient's medical records. The physician is the subject in the process, who is a part of the hospital community together with other stake-holders, each of whom has read, write or other responsibility of their own. The object at hand is patient's medical record, which has to be accessed by the physician. The task of accessing the record is governed by a set of rules, some explicit like access method and some implicit like hospital standards. The physician uses a set of obligations (tools) to gain the access, like an over-the-network login.

When we design a policy specification for the support of the above task, we include information about the physician in the <Subject> element, about the hospital setting in the <Environment>, aspects regarding the patient's medical record in the <Resource> element, and regarding the read responsibility towards the resource in the <Action> element of the <Target>. The conditions are part of the <Rule> element, and the tools are a part of the <Obligation> element of the <Policy>. Since they are not made visible in this scenario, they are not included in the policy specification.

Next, we design policy specification for the "organizational interconnectedness" within the workflow. Consider as an example, a physician is requesting a read access to patient's diagnosis from the researcher in the laboratories. The physician and the researcher are the subjects in the process, within the hospital and the research lab community, each of whom has access rights of their own. The object at hand is patient's diagnosis. Activity Theory allows to break down the workflow into separate activity systems. Each activity system is specified as detailed previously. The policies for each activity system are evaluated within its organization in the workflow. The overall outcome of the workflow is based the outcome of each of the two activity systems. If both policies are met then the diagnosis data flow is successful.

<table>
<tr><th colspan="5">Table 2. Case Application</th></tr>
<tr><th rowspan="2">Authorization Process</th><th colspan="3">Mapping Activity System to Policy System</th><th rowspan="2">XACML Policy – Transitive Workflow</th></tr>
<tr><th>Activity System</th><th>Data</th><th>Policy System</th></tr>
<tr><td>Physician can read/write patient data in hospital setting</td><td>Subject
Object
Responsibility
Community</td><td>Physician
Patient data
Read
Hospital</td><td>Subject
Resource
Action
Environment</td><td rowspan="2"><Policy id=”Workflow”>
<Policy id=”Activity”>
<Target>
<Subject>Physician</Subject>
<Resource>Patient Data</Resource>
<Action>Read</Action>
<Environment>Hospital</Environment>
</Target>
</Policy>
<Policy id=”Activity”>
<Target>
<Subject>Underwriter</Subject>
<Resource>Patients Data</Resource>
<Action>Read</Action>
<Environment>Insurer</Environment>
</Target>
</Policy>
</Policy</td></tr>
<tr><td>Underwriting agent can read patient data in insurance setting</td><td>Subject
Object
Responsibility
Community</td><td>Underwriter
Patient data
Read
Insurer</td><td>Subject
Resource
Action
Environment</td></tr>
</table>

Conclusion

Access control models safeguard patient’s privacy consent by mitigating the risks of unauthorized access. In this model, a resource is governed by one or more policies that specify attributes required for obtaining access. However, the complexity of the healthcare system owing to the transitive nature of health workflows has made it difficult to define and implement access control policies. As a solution to this problem, in this paper, we provide a theory-driven methodology to enable the formalization of access control policies.

We have seen that Activity Theory is helpful for understanding the authorization process. Besides, it is an effective guide for the implementation of the policy and paves the way for the development of analysis tasks. The components of Activity Theory directly maps onto the policy model. Activity Theory therefore constitutes a perfect framework which underpins access control policy specification. The findings lead to the proposal of Activity Theory being adopted as a framework which underpins patient’s privacy consent in hospitals and other healthcare institutions.

In this research-in-progress paper, we focus on patient’s privacy consent in a complex healthcare setting, and address the research question: how to clearly define and implement access control policies in a transitive healthcare workflow? We extend Activity Theory to include “organizational interconnectedness” within transitive workflow, and propose a methodology for specifying access control policies. This paper therefore is a step in understanding the patient’s privacy consent and authorization in complex situations. We also suggest implications for policy designers to better specify access control policies by analyzing the security components and their interactions.

Our methodology can be extended in multiple ways: We believe that our methodology can help develop solutions that facilitate secure sharing of electronic health records. Furthermore, our adaptation of Activity Theory to include organizational interconnectedness can also be applied to other inter-organizational settings that involve the flow of information from one organization to the other. Our paper has limitation in that we focus only on XACML standard for policy specification.

Acknowledgements

The authors would like to thank the reviewers for their critical comments that have greatly improved the paper. The authors would also like to thank Kavita Narwani for her comments and contributions. This research is supported in part by NSF Grant No. 0916612 and 1241709. Usual disclaimer applies.

Reference

Anderson, A., Parducci, B., Adams, C., Flinn, D., Brose, G., Lockhart, H., Beznosov, K., Kudo, M., Humenn, P., Godik, S., Andersen, S., Crocker, S., & Moses, T. (2003). Extensible Access Control Markup Language (XACML) Version 1.0. OASIS Standard.

Azhar, A., Amin, M., Nauman, M., & Shah, S. (2012). Efficient selection of access control systems through multi criteria analytical hierarchy process. In Emerging Technologies (ICET) 2012 (pp. 1-8). IEEE.

Bertelsen, O., & Bodker, S. (2003). Activity Theory, In J. M. Carroll (Ed.), HCI Models, Theories and Frameworks: Towards a Multidisciplinary Science. San Francisco, Mogan Kaufmann: 291-324

Boer, N., van Baalen, P.J., & Kumar, K. (2002). An Activity Theory Approach for Studying the Situatedness of Knowledge Sharing. The 35th Hawaii International Conference on System Sciences, Hawaii, 2002.

Busch, M., Koch, N., Masi, M., Pugliese, R., & Tiezzi, F. (2012). Towards model-driven development of access control policies for web applications. In Proceedings of the Workshop on Model-Driven Security (p. 4). ACM.

Chaudhury, A., Mallick, D., & Rao, H. R. (2001). Web channels in e-commerce. Communications of the ACM, 44(1), 99-104.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. (2013). Data Model Development For Fire Related Extreme Events: An Activity Theory Approach. MIS Quarterly, 37(1).

De la Rosa Algarin, A., Demurjian, S., Berhe, S., & Pavlich-Mariscal, J. (2012). A security framework for XML schemas and documents for healthcare. In Bioinformatics and Biomedicine Workshops (BIBMW) 2012 (pp. 782-789). IEEE.

Engeström, Y. (1987). Learning by Expanding: An Activity-Theoretical Approach to Developmental Research Orienta-Konsultit, Helsinki, 1987.

Engeström, Y. (1999). Activity Theory and Individual and Social Transformation, in: Perspectives on Activity Theory, R.M.a.R.P. Engeström (ed.), Cambridge University Press, Cambridge, UK, pp. 19-38.

Foorthuis, R., Brinkkemper, S., & Bos, R. (2008). An Artifact Model for Projects Conforming to Enterprise Architecture Springer, 2008.

Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2003). Role-based access control. Artech House.

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98). ACM.

Hevner, A., March, S.T., Park, J., & Ram, S. (2004). Design Science Research in Information Systems," MIS Quarterly (28:1) 2004, pp. 75-105.

Huang, H., & Kirchner, H. (2011). Formal specification and verification of modular security policy based on colored Petri nets. Dependable and Secure Computing, IEEE Transactions on, 8(6), 852-865.

Kofod-Petersen, A., & Cassens, J. (2006). Using activity theory to model context awareness. In Modeling and Retrieval of Context (pp. 1-17). Springer Berlin Heidelberg.

Margheri, A., Masi, M., Pugliese, R., & Tiezzi, F. (2013a). A Formal Software Engineering Approach to Policy-based Access Control. Univ. Firenze, Tech. Rep.

Margheri, A., Masi, M., Pugliese, R., & Tiezzi, F. (2013b). On a formal and user-friendly linguistic approach to access control of electronic health data.From eprints.imtlucca.it, 263-268.

Milutinovic, S. (2008). The need for the use of XACML access control policy in a distributed EHR and some performance considerations. Medical and Care Compunetics 5, 137, 346.

Nardi, B. (1995). Activity Theory and Human-Computer Interaction, In B. A. Nardi (Ed.), Context and consciousness: activity theory and human-computer interaction: MIT Cambridge, MA, USA.

Nita-Rotaru, C., & Li, N. (2004). A Framework for Role-Based Access Control in Group Communication Systems. In ISCA PDCS (pp. 522-529).

Peffers, K., Uunanen, T., Rothenberger, M., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research," Journal of Management Information Systems (24:3), pp. 45-77.

Purao, S., Baldwin, C., Hevner, A., Storey, V., Pries-Heje, J., Smith, B., & Zhu, Y. (2008).The Sciences of Design: Observations on an Emerging Field, Communications of the AIS (23:29).

Reddivari, P., Finin, T., & Joshi, A. (2005). Policy-based access control for an RDF store. In Proceedings of the Policy Management for the Web workshop (Vol. 120, No. 5, pp. 78-83).

Sandhu, R., Coyne, E., Feinstein, H., & Youman, C. (1996). Role-based access control models. Computer, 29(2), 38-47.

Sanchez, M., Lopez, G., Gomez-Skarmeta, A., & Canovas, O. (2008). Using Microsoft Office InfoPath to Generate XACML Policies. In E-Business and Telecommunication Networks (pp. 134-145). Springer Berlin Heidelberg.

Shanker, D., Agrawal, M., & Rao, H.R. (2009). Emergency response of Mumbai terror attacks: An activity theory analysis, In Proceedings of ICSCF 09, Kochi, India

Tremblay, M., Hevner, A., & Berndt, D. (2012). Design of an information volatility measure for health care decision making. Decision Support Systems, 52(2), 331-341.

Uden, L. (2007). Activity theory for designing mobile learning. Inter. J. of Mobile Learning and Organization, 1, 81-102

Valecha, R., Upadhyaya, S., Rao, R., & Keepanasseril, A. (2012). An Activity Theory Approach to Leak Detection and Mitigation in Personal Health Information (PHI).Proceedings of WISP 2012. Orlando, FL.

Yin, R. K. (2014). Case study research: Design and methods. Sage publications.

Zhang, P., & Bai, G. (2005). An Activity Systems Theory Approach to Agent Technology," International Journal of Knowledge and Systems Sciences (2:1) 2005, pp. 60-65.