Incorporating Policy-Based Authorization Framework in Audit Rule Ontology for Continuous Process Auditing in Complex Distributed Systems

Numanul Subhani and Robert Kent

School of Computer Science, University of Windsor
401 Sunset Ave, Windsor, Ontario N9B 3P4
{hoque4,rkent}@uwindsor.ca
http://www.uwindsor.ca/cs

Abstract. Complex distributed information systems that run their activities in the form of processes require continuous auditing of a process that invokes the action(s) specified in the policies and rules in a continuous manner. A shared vocabulary, or common ontology, used to defined the processes, and the audit rule ontology for processes or modules are integrated to form a hybrid ontology that supports the acquisition and evolution of ontologies. A methodology to construct a Common Ontology and an audit rule ontology by coupling to an expert system for Continuous Process Auditing (CPA) has been introduced recently. In this paper, we present a policy-based authorization methodology incorporating Audit Rule Ontology for CPA within distributed audit rule ontology. We also propose the use of probabilistic risk determination and evaluation of risk level, along with access history heuristics that define the adaptable access control policies before making policy decisions.

Keywords: Policy-based Authorization, Continuous Process Auditing, Audit Rule Ontology, Authorization and Access Control, Semantic Web, Risk-Adaptive Access Control (RAdAC).

1 Introduction

Auditing encompasses a variety of methods used to measure and assess the compliance of a system to defined rules and policy guidelines. Auditing is just one facet of a more extensive set of processes, often rooted in accounting, intended to support assurance that the system is functioning as intended. Auditing is applied in many domains, such as government, business, education and health care, among others. Underscoring the breadth of auditing applications is the fact that most auditing is still performed by human agents, trained and experienced in many aspects of evidence gathering, interpretation of rules and guidelines, and clarifying of final reports in respect of limitations.

Increasingly, complex systems have grown beyond the capacities of human driven auditing to perform meaningful audits in a timely fashion that serves

R. Meersman et al. (Eds.): OTM 2014 Workshops, LNCS 8842, pp. 367–376, 2014.

stakeholders and oversight bodies. Such systems encompass networks of human agents and also highly automated software systems with semi-autonomous subsystems, all of which are assumed to be vulnerable to risk. Researchers have focused attention on automating significant parts of auditing, both as embedded components within systems working autonomously, and as decision support components serving human analysts.

One vital element throughout auditing concerns knowledge, namely, its acquisition, interpretation and uncertainty, or vagueness, in reasoning. Auditing practice dictates that meaningful definitions must be determined and documented; for the system components and processes to be audited, evaluation measures, rules and actions to be applied, and limitations or constraints must be expressed. Auditors must work with suitable knowledge expressed in natural language terms for human consumption, but also expressed in terms appropriate for application and reasoning through computational logic. In Continuous Process Auditing (CPA) methodology, an audit rule sheet is defined for each process or module. The matter of continuity of application in CPA ranges from continuous time-dependent modeling to discrete time steps of audit application adapted to application requirements through use of coarse-grained analysis of sub-systems, and estimation techniques based on limited rule sets. This consideration is used to determine the degree of conceptualization as knowledge, audit measures using sensors and reasoning through rules and inference.

Knowledge is an essential part of most Semantic Web applications and ontology, which is a formal description of concepts or classes in a domain of discourse [1], is an essential approach for structuring the knowledge. Extracting knowledge from text in a semi-automatic way and identifying effective procedures for achieving useful and reliable results are challenging research areas. In auditing applications, most rules are defined in the context of human understanding and language and can be used to support human cognitive reasoning and inference. Ontology-based reasoning has known shortcomings and limitations compared with rule-based reasoning [2]. To represent inferential knowledge, ontology alone is insufficient [3]; but, inferential rules are an essential part of the knowledge in an audit rule ontology for a process or module in CPA for real-time Decision Support systems [4]. Though chronological, topological, and other types of semantic relations already exist [5], within these methods only hierarchical concepts are extracted and reduced sets of semantic relations are in use.

Many systems, such as health care and government, are complex and heterogeneous in nature and their data sources are semantically heterogeneous. A common ontology approach is straightforward for dealing with homogeneous semantic data sources. Hybrid approaches and multiple ontologies to deal with the heterogeneity problem of ontologies have been discussed [6, 7]. Recently, we proposed a hybrid audit rule ontology approach that couples with an expert system to infer new relations from the existing concepts [8]. In autonomous pervasive distributed systems (e.g. hospital, nuclear power plant, manufacturing), accessing authorized data in real-time and enforcing data security as highly encrypted-

sensitive data are transported from one layer to another in various geographic locations are essential issues to handle before CPA is deployed.

Determination of security risk and evaluation of risk level are critical issues in evolving complex distributed systems. Demand for generating adaptable access control policies that use previous knowledge of access history and acceptable risk level is on the rise, especially in cloud-based distributed systems. The objective of this paper is to present an authorization and access control mechanism for audit rules along with a risk-adaptive policy based authorization framework for Continuous Process Auditing. The rest of the paper is organized as follows. Audit rule ontology and its hybrid layered construction approach are briefly discussed in section 2. A general discussion of the authorization and access control of continuous process auditing in the context of audit rule ontology is provided in section 3. Our proposed Policy-based authorization framework incorporating with audit rule ontology for any autonomous pervasive distributed systems is presented and illustrated using an use-case scenario in section 4. Finally, conclusion and future research directions are drawn in section 5.

2 Audit Rules and Ontologies

Following Gruber, an ontology is an explicit specification of conceptualization [1], that can serve as an effective and powerful tool to capture, store and work with domain knowledge in knowledge-based information systems. In terms of knowledge representation, there are several types of ontology, including high-level, generic, domain and application. Domain ontologies are intended to specify conceptualization of particular real-world domains and processes, such as finance or industries involved in the production or delivery of goods and services. In this section we describe the ontology aspects relevant to processes, then audit rules and finally hybrid approaches.

2.1 Process Ontology (PO)

All activities in a process are linked as sequential steps, either defined by higher business modelers or discovered by various established methodologies, such as workflow mining from labeled and unlabeled event logs, stochastic workflow analysis or rule-based approaches. There are two approaches to the study of any system and its behavior: the micro system (μ), which studies the algorithms, sensors for collecting data, and atomic devices; and the macro system (M), which studies and models large systems composed of large numbers of algorithms, devices and connections [8]. Process Ontologies (PO) are constructed for each process with their defined concepts and databases that might be either homogeneous or heterogeneous in nature, and an expert system for PO mappings is coupled to construct a hybrid layered ontology for process audit rules.

2.2 Audit Rules and Audit Rule Ontology of a Process (AROP)

As a first step, audit rules are defined for an activity or component within the scope of human-performed auditing. Audit rules are based on both the

hierarchical structure of an organization and the enforced business controls. The same audit rules discernment and definition approach can be applied and implemented in any Continuous Process Auditing system where a process has to traverse through various components, and by applying audit rules sequentially through the traversal. An Audit Rule Ontology for a Process (AROP) may be used to detect exceptions to the audit rules in a process during CPA. Semantic rule-based reasoning can facilitate construction of AROP in a semi-automatic way. AROPs would be used as second layer under common ontology in a hybrid layered ontology model. We assume that human approval of all audit rules is enforced; autonomous automated approval through artificial intelligence is not considered in this discussion.

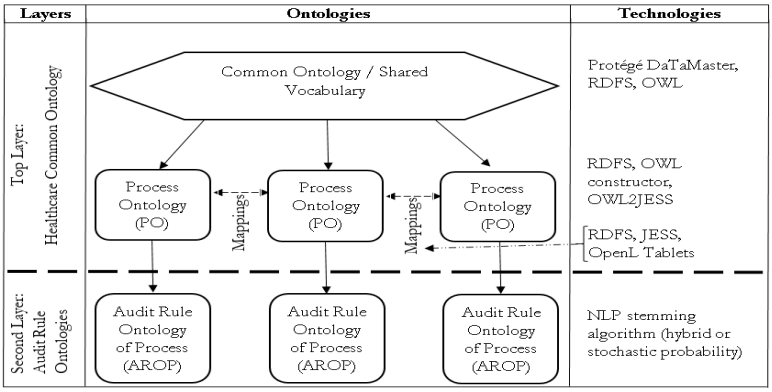

Fig. 1. Conceptual Model of Hybrid Audit Rule Ontology

2.3 Ontology Design: A Hybrid Layered Model

Domain ontologies may be divided into linguistic and conceptual ontologies. According to Gruber [1], Conceptual Ontologies (CO) represent the domain objects, distinguishing between the primitive concepts and the defined concepts, whereas Linguistic Ontologies (LO) define words or contextual usages of words. The Process Ontology (PO) contains only the defined concepts and the Mapping Ontology (MO) contains both the defined and the underlying primitive concepts. The observation in [9] led to identifying some relationships between POs, MOs and LOs. Mappings between POs may be defined in terms of equivalence operators of some MO. The various meanings of words in MO references may be defined by LOs and this reference would provide a basis for formal, and exact or uncertain reasoning, and automatic translation of context-specific terms.

In our proposed single common ontology approach to domain ontology construction each PO is attached to a database that might be heterogeneous in nature with other databases. Each PO describes the semantics of data sources individually. Inter-PO mapping is realized by the MO, which is defined with

primitive concepts. The simplicity and flexibility permitting addition of new sources (like new POs) with little or no need of modification, is the main advantage of this mechanism. To integrate several POs addressing the same domain, this mechanism exploits the MO's capability to define equivalent and similar concepts.

As detailed by Wache [6], one develops the Common Ontology using multiple POs in the top-most layer, then Audit Rule Ontologies of Processes would be stemmed as a second layer under the top-most layer to form a Hybrid Layered Ontology. Fig. 1 visualizes the conceptual model of both the layers alongside with the technologies to be used to integrate and develop the entire operable Audit Rule Ontology system. More abstract description of construction, development and operational mechanism are discussed in [8].

3 Authorization and Access Control of Continuous Process Auditing

A Continuous Process traverses through multiple modules or micro processes [8] and it requires seamless access control to all data sources in a complex distributed system for assessing audit rules. Different stakeholders, actors and networking modules that are part of a process need various levels of authorization policies for access control. In distributed environments, it is daunting challenging task to provide authorization and access control and many different mechanisms have been investigated. Most distributed systems employ numerous policies to provide authorization for access control. Policy based authorization mechanism is being investigated [10–12] and the policy conflict resolution problem has yet to be addressed while eliminating real-time performance bottlenecks.

Organizations are constantly evolving. Thus, the authorization policies that guide them must also be adaptable and extend to a variety of risk factors. In audit rule ontology, a CPA requires all the authorization policies to access control of all data sources for each module, or micro process, before assessing the audit rules. Assessing audit rules that deal with a variety of audit risks is one of the major access control requirements as well within AROP. Since common ontology lies on top of all ontologies (Fig. 1), its audit rules require the access control and authorization policies to all data sources of common ontology; the same is true for the all other ontologies in 2nd and 3rd layers of ontologies as well.

To gain the access control and authorization policies of all data sources in different layers of ontologies, we proposed a policy-based authorization framework incorporating with AROP and we also devised a modified Risk-Adaptive Access Control (RAdAC) model [13] to enforce adaptable and risk-aware access control in any complex distributed system, particularly in real-time.

4 Policy-Based Authorization Framework Incorporating with Audit Rule Ontology

In Section 2.3, we proposed the hybrid ontology for Audit Rule Ontology for Process. A Process traverses through Common Ontology first, then Process

Ontology before reaching to AROP. An Audit Rule Ontology of Process (AROP) is constructed with audit rules obtained from two layers of ontologies i.e. Common Ontology and Process Ontology (Fig. 1). Process ontologies are mapped in-between by Mapping Ontology. Authorization Policies are also deployed and enforced along with the ontologies in their nodes. Polices must be defined incorporating with the ontological predicates. Common authorization policies that have to applied/enforced for all the branches of ontologies must be deployed and enforced in Common Ontology and same way process specific authorization polices must be deployed and enforced in Process Ontology. After getting authorization from CO and PO, Audit Rule Authorization Polices (ARAP) are also enforced in AROP. Before making decision and providing access to the access control for data access layer, ARAP must adjust or adapt to the security risk (automatically or semi-automatically) to resources associated with that process and audit rule. Below we have described the framework of RAdAC using Audit Rule Ontology for Process.

4.1 Audit Rule Authorization Policy (ARAP)

Audit Rule Authorization Policies define the process goals of the system and event triggered reactions from the policies in order to deal with them. Events are produced, or may be produced some time in future, by receiving a message from an ontology object within the system. There are currently two basic policy types defined: Obligation Policies and Authorization Polices. Obligation Polices specify the actions that must be performed by CO and PO within the system when certain events occur and provide the ability to respond to changing circumstances. Authorization Polices are essentially access control policies, to allow or deny message passing between objects (ie. resources and services).

4.2 Risk Determination and Evaluation

Probabilistic determination of the security risk associated with granting the requested access is made based on examining several external factors. The level of risk is calculated from several areas such as the risk associated with the users, protection capabilities and robustness of system components, the operating threat level of the environment and access history. We only define the user (as an entity that is requesting access) and connection (as any communication channel on the users device) to capture the security risk. In future, we plan to consider the risk of device, associated components, operational matter, service provider's trustworthiness and the risk level assurance. This process provides quantitative indication of the level of risk and the risk evaluation on risk associated with each of these components as well as heuristics described below.

4.3 Heuristics of Access History and Acceptable Risk Level

Knowledge of the past access control decisions help to fine-tune the access control policy to improve the rate of positive access control decisions and can be used to

develop better algorithms for determining risk. Policy must specify the degree to which heuristics should be considered in each access decision, as well as how each decision should be incorporated into the learning process. The policy will have to specify an acceptable risk level for each area, or a risk range. We consider access history and acceptable risk level to capture the characteristics of heuristics. It updates the object access history repository with acceptable risk level in the access request and the access control decision, then it provides access for making future access decisions.

4.4 Adaptable Access Control Policies

This specifies the rules for access control for various classes of information objects under different conditions. The purpose of adaptable access control policies is defined to capture an audit rule's need to access an object. User and connection are defined to capture the security risk. Access history and acceptable risk level are defined to provide feedback to the access decision process and to capture the access decisions. Since our main purpose is to access for audit rule, we did not consider including overriding process where an allowed authority can override an access decision made by the system under specific conditions.

4.5 Policy Decision and Post Processing

A Policy Decision sequence is defined by: (a) ARAP defined by specifying the heuristics and acceptable level degree of risk, (b) determining security risk as a quantifiable amount then evaluating security risk with heuristics knowledge of access control decision and acceptable risk level, (c) capturing the access control decision and acceptable risk level to update the object access history repository then providing access for making future access decisions. This heuristics step gives feedback to the "risk determination and evaluation" and to define the "adaptable access control polices" steps as well, and lastly, (d) decision making and post decision processing. Complete policy decision sequence flowchart is presented in Fig 2.

Post decision processing, among other tasks, is aimed at supporting the need for access control to filter out the authorized data from the data access layer based on the access decision. Various tools are available to filter out data from the data access layer; we are considering XACML to do this job in the following two ways: (a) filtering authorized data returned from data sources, and (b) modifying input parameters according to the authorization before retrieving the data from data sources. In typical complex distributed systems, there are a large number of data sets to filter out. We adopt the approach of modifying the input parameter, and are investigating if this is the preferred approach. Associated with this matter is how to manage efficiently frequently accessed authorization data for making decision in near real-time.

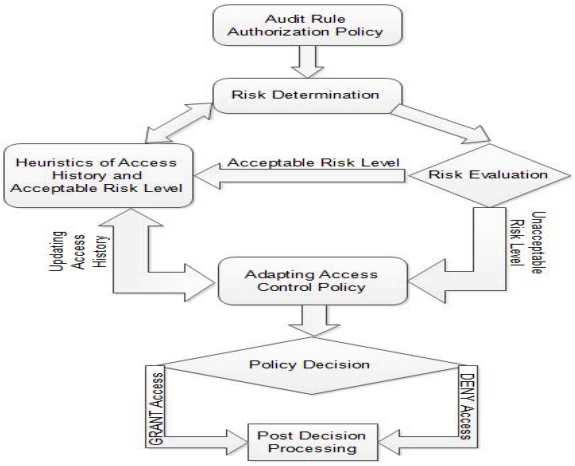

Fig. 2. Conceptual Model of Audit Rule Ontology based Risk-Adaptive Access Control Framework

4.6 Use-Case Scenario for an Audit Rule Authorization Policy

An example of Risk-Adaptive Access Control Framework (RAdAC) is illustrated in the following as sequential steps from audit rule authorization policy towards granting or denying access to services aor resources for a facility management system. In this scenario, Alice is a junior employee working in the IT department of a firm, within a team led by John, who has placed Alice under the supervision of Mark, a senior member of Johns team. To aid in identifying mistakes made due to unauthorized access, a continuous audit system should be capable of capturing and analyzing non-compliance with established policies, especially in cases where such policies may apply only after deriving a reasonable and consistent inference.

1. ***Authorization Policy:*** An audit rule authorization policy that defines the goal of approving contract worker overtime might be stated as: Allow contract worker to work overtime maximum of 6 hours. A contract worker overtime process definition (including working condition, payment method, overtime rate, work shift schedule, worker specific contract terms, etc.) should be clearly defined in the process ontology of a contract worker overtime module. This authorization policy governs the access control of providing and using services, and using resources by contract workers. As an example, Alice, a contract worker, is hired as an electrician to work only in morning shift under Marks supervision. Should Alice be given access to work overtime in the server room in midnight shift without any supervision?
2. ***Risk Determination and Evaluation:*** Determining the risks associated with granting Alice the requested access is made probabilistically by examining several external factors such as Alices security clearance level, the operating threat level of environment, access history and so on. As mentioned earlier, we consider only a user as an entity and a connection as a

communication channel on the user device to calculate the level of risk. Each component (for Alice only entity and connection) relating to granting of requested access is equipped with appropriate tools or devices to calculate the level of risk. Acceptable Threshold level of risk is determined by the authorization policy from audit rule ontology. For instance, if the entity risk level is 4 and connection risk level is 8, and for Alice, acceptable entity risk threshold level is 3-5 and connection threshold level is 4-7, authorization to access should not be granted.

3. ***Heuristics of Access History:*** Since Alices connection risk level is not within the threshold level, the audit system needs to adapt an access control policy for Alice by using heuristics of her access history along with acceptable risk level. By examining the access history, Alice was given access 5 times to the server room manually by her supervisor Mark with connection risk level 8, three times under his own supervision in the morning shift and two times under supervision of team leader John, who is Marks supervisor, in the midnight shift. After analyzing the access history and acceptable risk level for Alice, heuristics pointed out two facts: (a) all 5 times Alice was given access to the server room under an employee supervision (assume both Mark and John have security clearance level 3, and John is superior to Mark) that has required security clearance 3, and (b) this time Alice is requesting access without supervision
4. ***Adapting an Access Control Policy:*** Based on the heuristics, facts and level of risk associated to granting the requested access, an access control policy must be adapted that Alice can be given the requested access under supervision by an employee with level 3 security clearance.
5. ***Decision Making:*** Since Alice was always supervised by an employee with level 3 security clearance and she is now seeking access without supervision, then she should NOT be given access to the server room.

Although Alice was given access to the server room several times earlier with supervision, the security risk associated with entity, connection, and the knowledge of the past access control decisions aided the RAdAC system to adapt an access control policy for similar kind of events without any intervention from human administrators.

5 Conclusion and Future Work

We have presented a conceptual policy-based authorization framework incorporating audit rule ontology. This framework adapts the modified version of Risk-Adaptive Access Control (RAdAC) with the security risk components of users and connections between devices. We believe that policy-based authorization framework with modified RAdAC in Audit Rule Ontology for Process (AROP) addresses real world scenarios where risk in an important factor in Continuous Process Auditing and making access control decisions.

In future, we will include more security risk components such as the risk of device, associated device components, operations, service provider trustworthiness

and risk level assurance. We plan to use the heuristics of user security history, and service provider's risk level of asserted algorithmic and authentication strength as well. A resolution mechanism for policy conflict will be addressed as well in future extensions of this framework.

Acknowledgment. We acknowledge support from the Canadian Institutes for Health Research (CIHR).

References

1. Gruber, T.: A translation approach to portable ontology specifications. Knowledge Acquisition 5(2), 199–220 (1993)
2. Horrocks, I.: Daml+oil: A description logic for the semantic web. IEEE Data Engineering 25(1), 4–9 (2002)
3. Harmelen, F., Fensel, D.: Practical knowledge representation for the web. In: Proc. 16th Int'l Joint Conf. Artificial Intelligence (1999)
4. Baksa, R., Turoff, M.: Continuous auditing as a foundation for real time decision support - implementation challenges and successes. Annals of Information Systems Supporting Real Time Decision-Making 13, 237–252 (2011)
5. Valencia-Garcia, R., et al.: An incremental approach for discovering medical knowledge from texts. Expert Systems with Applications 26(3), 291–299 (2004)
6. Wache, H., et al.: Ontology-based integration of information - a survey of existing approaches. In: Proceedings - IJCAI Workshop, pp. 108–117 (2001)
7. Klein, M.: Combining and relating ontologies: an analysis of problems and solutions. In: Proceedings - IJCAI Workshop, pp. 53–62 (2001)
8. Subhani, N., Kent, R.: Novel design approach to build audit rule ontology for healthcare decision support systems. In: International Conference on E-Learning, E-Business, Enterprise Information Systems, and E-Government, pp. 133–138 (2014)
9. Jean, S., Pierra, G., Ait Ameur, Y.: A domain ontologies: A database-oriented analysis. In: Jean, S., Pierra, G., Ait-Ameur, Y. (eds.) WEBIST 2005/2006. LNBIP, vol. 1, pp. 238–254. Springer, Heidelberg (2007)
10. Twidle, K., Dulay, N., Lupu, E., Sloman, M.: Ponder2: A policy system for autonomuous pervasive environments. In: International Conference on Autonomic and Autonomous Systems, pp. 330–335 (2009)
11. Singh, S., Singh, K., Kaur, H.: Design and evaluation of policy based authorization model for large scale distributed systems. IJCSNS International Journal of Computer Science and Network Security 9(11), 49–55 (2009)
12. Cao, J., Chen, J., Zhao, H., Li, M.: A policy-based authorization model for workflow-enabled dynamic process management. Journal of Network and Computer Applications 32(2), 412–422 (2009)
13. Kandala, S., Sandhu, R., Bhamidipati, V.: An attribute based framework for risk-adaptive access control models. In: Availability, Reliability and Security (ARES), pp. 236–241 (2011)