

SemPIF: A Semantic Meta-Policy Interchange Format for Multiple Web Policies

Yuh-Jong Hu
Dept. of Computer Science
NCCU, Taipei, Taiwan
hu AT cs.nccu.edu.tw

Harold Boley
IIT – e-Business,
NRC-CNRC, Canada,
Harold.Boley AT nrc.gc.ca

Abstract—We propose a semantics-enabled layered policy architecture (“policy layer cake”) for the exchange and management of multiple policies created by different policy languages on the Web. This architecture consists of four layers: Unifying Logic layer, Policy Interchange Format (PIF) layer, Privacy Protection/DRM layer, and Domain Specific Applications layer. A meta-Policy Interchange Format (meta-PIF) layer is also introduced, side by side with the corresponding PIF layer, allowing a facilitator to provide uniform services of interchange, reconciliation, and combination of multi-policies from various domains on the Web. This SemPIF¹ architecture extends W3C’s Semantic Web architecture to permit the reuse of earlier work. A use case scenario of a facilitator employing SemPIF for multiple DRM and privacy protection policies on digital library subscription services will be demonstrated.

Keywords—semantic web; ontology and rule; computer policy; privacy protection; digital rights management;

I. INTRODUCTION

The current Web, i.e. Web 1.0, has been extended toward the *Semantic Web* and also toward the *Social Web*, i.e. Web 2.0, where the *Social Semantic Web* combination of both extensions is sometimes called Web 3.0. In the Semantic Web and Web 3.0, information is given well-defined meaning to better enable computers and people to work in cooperation. The well-known Semantic Web layered architecture² has undergone revisions reflecting the evolution of layers such as the Description Logic (DL)-based ontology language OWL [1], the Horn Logic (HL)-based rule language RIF [2], and their relationship.

On the other hand, policy languages, such as Rei [3], KAoS [4], Protune [5], have also been proposed – on the basis of ontology languages and rule languages – to allow agents understand policies and to enforce these policies as intended by their semantics. However, the semantic bases of policy languages vary considerably, ranging from DL to HL to Logic Programming (LP), e.g. leading to different stances w.r.t. the unique name assumption (UNA) and the closed world assumption (CWA) [6]. This makes multiple policies created in these policy languages hard to interchange and to combine with each other.

In [5], Policies are formulated and treated as knowledge bases, i.e. ontologies and rules. Thus, many operations can be automated, thereby reducing ad-hoc program coding to a minimum and enabling automated documentation. Policy framework also need to support interoperability. Moreover, the context of policy itself is described in a machine understandable way.

Therefore, we propose a semantics-enabled policy architecture consisting of four layers: Unifying Logic (UNL) layer, Policy Interchange Format (PIF) layer, Privacy Protection/DRM (PPD) layer, and Domain Specific Applications (DSA) layer. Here UNL directly corresponds to the layer “Unifying Logic” of the most recent version of the Semantic Web architecture. We also introduce a meta-Policy Interchange Format (meta-PIF) layer, side by side with the corresponding PIF layer, allowing a facilitator to provide the management functions of interchange, reconciliation, and combination of multi-policies from various domains on the Web. The Policy Web architecture can be viewed as an extension of the Semantic Web architecture, as shown in Figure 1.

PIF is based on DL-based ontologies and LP-based rules, e.g. ontologies+rules that allows a facilitator to use PIF to support basic interchange services of multi-policies created from different policy languages. In addition, we may use meta-PIF to specify meta-policies for managing multi-policies created either from PIF or other policy languages. Meta-policy was shown to be a policy about policies that provides a set of rules for enforcing the adding/changing management services of multi-policies. Moreover, meta-policy can be defined as a set of rules for setting up the priority of policies to coordinate, enforce, and even negotiate multi-policies on the Web [7].

In a particular policy language framework, policy management services could be done as meta-policies shown in Rei framework [3] or it could be implemented as policy administration tools shown in KAoS [4]. In the Protune’s framework, the role of meta-policies is in governing the behavior to reduce ad-hoc programming efforts and to improve policy readability and maintainability.

However, policies management services in these frameworks were only allowed to operate within their own environments. Therefore, we propose SemPIF to allow a facilitator to use meta-policies providing the management services of

¹SemPIF can be read as both Semantic PIF and Semantics-enabled meta-PIF.

²<http://www.w3.org/2007/03/layerCake.svg>

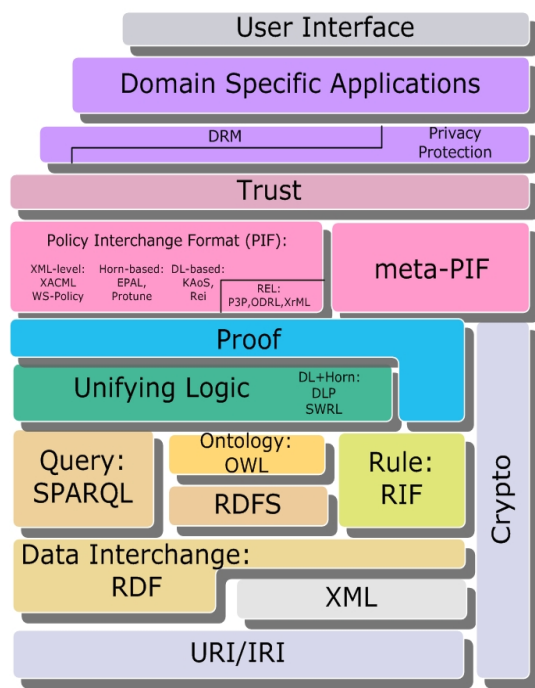


Fig. 1. SemPIF: a semantics-enabled layered policy model of semantic policy interchange format (PIF) and meta-PIF

policies interchange, combination, and even negotiation across multiple heterogeneous domains.

XML-based Rights Expression Language (REL) lacks of semantic expression power so it is a restricted form of policy language in the PIF layer. Currently, we have three RELs available, e.g. P3P for privacy protection and ODRL/XrML for DRM. Unfortunately, policies created from these XML-level RELs lack formal semantics, which prevents software agents from automatically and accurately interpreting and processing these policies on the Web.

A formal semantic policies model could be expressed and enforced as a ontologies and rules combination for DRM and privacy protection purposes. Obviously, if we do not know what the available expression features are of each ontologies+rules combination, we cannot decide which combination will be the best one representing formal semantics of RELs. We have shown the semantics of DRM policies for DRM in PPD as a homogeneous ontologies+rules combination of SWRL to structure the semantics of ODRL [8]. We also have shown that privacy protection policies with a heterogeneous ontologies+rules combination of DL+log in UNL formalize the semantics of P3P in PIF layer [9]. Without SemPIF, the semantic policy formalizing models cannot be used by a facilitator for exchange and reconciliation of multi-policies from various domains on the Web.

We will outline several issues in the designing of a meta-PIF, which allows a facilitator using SemPIF to interchange and transform of multiple privacy protection and DRM policies with different policy languages. We come up with some solutions to manage this problem.

Compared with other policy languages, such as KAOs, Rei, and Protune, PIF follows W3C ontology and rule standards, such as RIF RDF and OWL Compatibility [10] and strives to provide a mechanism for a facilitator to preserve different policies syntax and semantics throughout its integration and interchange of multi-policies. In addition, a facilitator can use meta-PIF, providing further management and reconciling services of PIF-enabled multiple policies across various domains.

Another insight of our investigation of the DRM vs. privacy usage control problem is: While DRM systems are collecting our personal information for usage control purposes, it is quite possible that they might also invade our privacy rights. To reconcile this conflict, the combination of ontology language and rule language in meta-PIF permit a facilitator to enforce the fine-grained mapping and merging of ontologies with interchangeable rules from multi-policies in privacy protection and DRM. This paves the way for accomplishing the objective of unifying multiple web policies through SemPIF.

Finally, we will show a use case scenario for digital library subscription services in a client server model and demonstrate how to use it via a facilitator, eliminating the possible conflicts between the server's DRM policies and the client's privacy protection policies.

II. RELATED WORK

REL is a subset of PIF layer. The FOL semantics-enabled policy models for RELs have been proposed to specify the semantics of ODRL, XrML, and P3P [11] [12] [13]. However, it is still unclear how to design semantics-enabled policy languages from these semantics-enabled RELs to allow their policies to be machine readable and understandable on the Web.

In terms of Semantic Web languages, Tonti et. al. have compared KAOs, Rei, and Ponder, three policy languages, in the representation and reasoning of specific policies [4]. In fact, the policy semantics of KAOs and Rei came from DL-based ontology concepts. We can have a policy management services framework for agents to manage their policies, such as Rei. However, agents still cannot inter-operate and cooperate with other agents across different frameworks. Moreover, policies created from rule-based policy language, such as Protune [5] were not able to inter operate and cooperate with these ontology-based policies either. Therefore, we need a *de jure* standard policy interchange language as with the work in the W3C PLING³ or in the OMG's SBVR⁴ or to use neutral policy interchange framework, i.e. SemPIF to achieve policies interoperability.

The idea of meta-policies were proposed almost two decades ago [7]. It was used for policy management services in the Rei and Protune frameworks [5] [3]. In Rei framework, authors tried to propose a policies interchange mechanism instead of using a single policy language for describing all

³Policy Interchanges Interest Group - PLING, http://www.w3.org/Policy/pling/wiki/Main_Page.

⁴Semantics of Business Vocabulary and Business Rules (SBVR), <http://www.omg.org/spec/SBVR/1.0/>.

multi-policies. This Rei framework's objective is close to our statements. In the Protune framework, the meta-policies provide a simple means to specify which parts of the policy are sensitive, and how application-specific atomic conditions are to be verbalized in the documentation. However, Rei and Protune frameworks did not show a semantics-enabled policy layered architecture like ours to be compatible with the current Semantic Web architecture.

III. SEMANTIC WEB LAYERED ARCHITECTURE

We have both web markup language and Semantic Web language in the Semantic Web Layered Architecture (SWLA) (see Figure 1). The XML/XML-Schema with IRI/URI is a web markup language that provides interoperable syntax for RELs at the PIF layer. The semantics of RELs need to be formalized as one of ontologies+rules combinations from the UNL, to structure the policy meaning. For Semantic Web languages, we have ontology language, rule language, and a combination of ontology language and rule language, i.e. (ontology+rule) language. The Ontology language includes graph-based RDF(S) and DL-based OWL. As for the Horn-based (or LP-based) rule language, it includes RuleML and RIF. SWRL is a Semantic Web language with a combination of OWL-DL ontology language and Datalog rules so it is an (ontology+rule) language [14]. The OWL 2 RL or its combination with RIF is another emerging (ontology+rule) language that can be compared with SWRL⁵.

A. Unifying Logic

PIF and Sem-PIF are based on the unifying logic of description logic (DL) ontologies and logic program (LP) rules [6]. In the Unifying Logic (UNL) layer, description logic (DL) is a subset of the First Order Logic (FOL). DL provides a basic logic foundation for an ontology language, such as OWL 2. Similarly, Horn logic (or LP) provides a basic logic foundation for rule languages, such as RIF or RuleML. One of LP's characteristics, e.g. procedure attachment is not included in the DL (or FOL) but this feature is very important for the execution of multi-policies' actions.

The DLP was shown as an intersection of DL and LP [15] but it has quite limited expression power when we compare it with other ontologies+rules combinations, such as AL-log, DL-log etc [16] [17]. The homogeneous ontologies+rules combination of DL and LP for DL+Datalog provides a basic logic foundation of SWRL.

These ontologies+rules combinations have much more powerful expressions of ontologies+rules than DLP for meta-PIF. However, we have not found which combination is the best for SemPIF's representations and enforcements and they did not have standardized XML syntax either to become Semantic Web languages shown in the SWLA.

⁵The combination of OWL 2 and RIF has been shown in <http://www.w3.org/2005/rules/wiki/OWLRL>.

B. Policy Interchange Format

In the Policy Interchange Format (PIF) layer, it consists of regular logic-based policy language, such as Rei, KAoS, Protune, EPAL [18], and an XML syntax policy language, such as XACML [19]. In PIF, Rei and Protune are the two frameworks which have their own meta-policies, providing simple policy management services for ordinary policies. Otherwise, policies management services can be referred to meta-PIF in the SemPIF architecture.

P3P and EPAL were proposed as policy languages for privacy protection in the corresponding client-server model and server-server model [20] [21]. As RELs sublayer, ODRL and XrML were proposed for designing policies of DRM [22] [23]. We have added DL-based or Horn-based logic as semantic primitives of these RELs to explicitly define semantics of these policy languages.

In this PIF layer, we have DL-based policy languages, such as Rei and KAoS; or Horn-based policy languages, such as EPAL and Protune to represent ordinary policies. A policy's explicit representation in terms of ontologies or rules depends on what the underlying logic foundation of your policy language is. If your policies are created from DL-based policy language, such as Rei or KAoS, then ordinary policies are shown as TBox ontologies schema and ABox instances. Otherwise, policies created from LP-based policy language, such as EPAL or Protune ordinary policies are a set of rules with predicates of unary, binary, or ternary variables and facts.

Based on our observations, these policy languages in the PIF layer did not fully utilize the OWL or RDF(S) syntax and semantics expression power shown in the SWLA. Therefore, we do not expect these policy languages to be fully compatible with their indicated ontology languages or rule languages. One of the important issues is multi-policies created from these different policy languages might not be able to interchange or negotiate with each other from various domain specific applications. Therefore, we need to use PIF and meta-PIF to achieve multi-policies interchange, combination, reconciliation, and negotiation.

C. Privacy Protection and DRM

Privacy protection and DRM are shown as independent but intertwined layers on top of PIF and meta-PIF (see Figure 1). This relationship reflects that access rights enforcements for these two domains are closely related with each other. In [24][25], authors proposed that the DRM system should consider user desirable privacy rights indicated in the Fair Information Principles (FIP), such as collection limitation, purpose disclosure, use limits, etc and enforce privacy protection policies. Otherwise, user privacy rights might be violated. Based on this idea, a use case scenario will be demonstrated in this paper to show how a facilitator can employ SemPIF to reconcile rights conflict from multiple DRM and privacy protection policies (see section V).

IV. SEMPIF FOR MULTIPLE WEB POLICIES

The research objective here is to use a suitable ontology+rules combination that represents the semantics of underlying XML-based rights expression languages (RELS) in the SWLA. Based on this ontology+rule language, a facilitator provides a sound and complete interchange mechanism to avoid possibly inconsistent or ambiguous semantics between source and target policies.

A. Meta-PIF

We consider the meta-PIF as a part of SemPIF architecture that can be used by a facilitator to provide management services of policies, including policy sequencing, adding, deleting, merging, changing, reconciling, and even resolving conflicts.

Original trust layer in the SWLA is between the PIF/meta-PIF and the PPD so a facilitator uses meta-policies created from meta-PIF to manage the PIF-based policies to represent and enforce the trust services criteria specified in the underlying Crypto.

We envision several important issues in the design of a facilitator while using SemPIF as a mediation architecture:

- In the SemPIF architecture, a facilitator uses PIF to provide basic interchange services of various policy languages. Moreover, a facilitator uses PIF to provide advanced policies interchange for a particular domain, which extended from PIF.
- In each PIF's policy header file, we have to specify the type of source policy language and its corresponding unifying logic to allow a facilitator to proceed with policies interchange services of a specific domain application. Certainly, we also import a specific domain ontology schema in the PIF's policy head file so that we can use this schema's vocabularies to describe the concepts of policies for a particular domain.
- The basic primitive vocabularies of PIF needed for interchange of policies are very concrete and the total number of them is also small. In fact, most of these basic primitive vocabularies have already been specified in the various REL policy languages, such as P3P or ODRL. They are: *principal*, *subject (owner)*, *object (user)*, *resource (or asset)*, *right*, *obligation*, *purpose*, and *condition*. However, access right expressions for privacy protection and DRM are different. For example, in a privacy protection domain, we have: *collect*, *retain*, *disclose*, etc access rights but in a DRM domain, we have: *download*, *view*, *print*, etc usage rights.
- The basic primitive vocabularies of meta-PIF are the same as PIF's except some of the basic primitive vocabularies in meta-PIF directly correspond to PIF-based policies. The policies are indicated as resource entities with respective users, rights, conditions, priority, etc for a facilitator to enforce its adding, deleting, merging, etc management services of policies.
- The meta-PIF is a meta-policy language of PIF and only provides management services for PIF-based policies.

If meta-PIF attempts to provide an interchange format of different meta-policies in PIF, then we also have to provide policy management interoperability services for different policy languages. Currently, we do not have so many meta-policy languages except Rei and Protune, so this function will be temporarily unnecessary.

V. A SCENARIO OF DIGITAL LIBRARY SUBSCRIPTION SERVICES

In a client server model, protection policies are created from various policy languages, such as ODRL, P3P, XACML, and EPAL for enforcing DRM and privacy protection. This access control scenario is extended from the use case of policy-aware access control for the open Web environment in [26]. A facilitator uses PIF-based policies to provide the services of interchange semantics-enabled protection policies between a client and a server or among servers. Moreover, a facilitator uses meta-PIF-based policies to manage these PIF-based policies, which permits clients and servers to compromise on their respective rights and obligations under some conditions (see Figure 2).

A. Web servers' policies

The NCCU university library has subscribed *IEEE*, *ACM*, and *Springer* digital library services, which provide a set of eJournal article's access rights for authorized students and staff. There are two categories of policy for a IEEE web server: one for DRM and the other for declaration of privacy protection. As an example of DRM policy, if the NCCU library is in an IEEE digital library subscription list, then an *IEEE* web server allows a certified user of the NCCU library to obtain accessing rights for a set of its digital articles. The other example is the IEEE publisher declares its privacy protection policy. Examples are shown as follows.

1) *Policies declared in the IEEE*: IEEE publisher has two PIF-based policies: *policy(drm1-IEEE)* for DRM and *policy(pp1-IEEE)* for privacy policy declaration, where *policy(?var)* indicates the policy name is bound to *?var*, which corresponds to a particular uri (uniform resource indicator) address as a resource for a facilitator to use meta-PIF-based policy to enable the policy management services. The following policies will be shown as either natural language or RIF policy, which predicates were declared in the PIF-based ontologies for privacy protection and DRM (see Figure 3 and Figure 4).

- *policy(drm1-IEEE)*:

policy as natural language:

If a student owns a valid student ID issued by a department of University, e.g., a registrar. A department of an University, e.g., digital library is one of a subscribers in a publisher list, then a student is endowed with DRM usage rights {download,view,print} of an eJournal from a web server of the IEEE publisher.

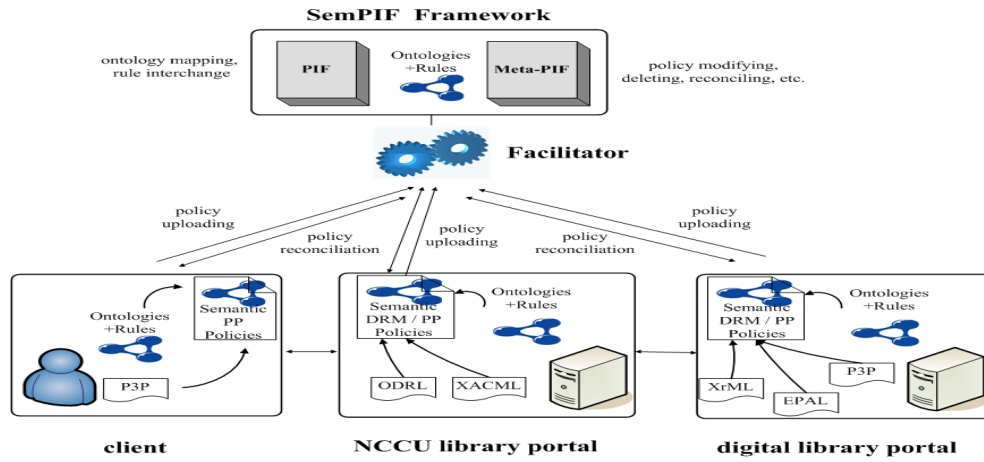


Fig. 2. A facilitator provides policy interchange services with PIF-based policies and policy management services with meta-PIF-based policies

policy as RIF:

$$\begin{aligned}
 & ?st\#Student\wedge?id\#StudentID\wedge?st[own \rightarrow ?id] \\
 & \wedge ?uni[hasPart \rightarrow ?rg]\wedge ?st[enrolledAt \rightarrow ?uni] \\
 & \wedge ?rg[issue \rightarrow ?id]\wedge ?uni[hasPart \rightarrow lib] \\
 & \wedge ?lib[subscribedTo \rightarrow IEEE] \\
 & \wedge IEEE[hasPublished \rightarrow ?ejr] \\
 & \wedge IEEE[endowedWith \rightarrow ?rgt] \\
 & \wedge ?rgt[appliedTo \rightarrow ?ejr] \wedge IEEE[delegate \rightarrow ?st] \\
 & \implies ?st[endowedWith \rightarrow ?d] \\
 & \wedge ?st[endowedWith \rightarrow ?v] \\
 & \wedge ?st[endowedWith \rightarrow ?p] \\
 & \wedge ?d\#Download\wedge ?d[appliedTo \rightarrow ?ejr] \\
 & \wedge ?v\#View\wedge ?v[appliedTo \rightarrow ?ejr] \\
 & \wedge ?p\#Print\wedge ?p[appliedTo \rightarrow ?ejr].
 \end{aligned}$$

- *policy(pp1-IEEE):*

policy as natural language:

If a person owns DRM usage rights from a web server of the IEEE's publisher and this publisher has a purpose of enforcing DRM control on collecting, retaining, and disclosing client person's data then the IEEE publisher is endowed with privacy usage rights {collect, retain, disclose} on this data, including profiles and digital traces in this a web server under the condition of retention period two months since the data are first collected.

policy as RIF:

$$\begin{aligned}
 & ?per[endowedWith \rightarrow ?drmr] \\
 & \wedge ?drmr[appliedTo \rightarrow ?ejr] \\
 & \wedge IEEE[hasPublished \rightarrow ?ejr] \\
 & \wedge IEEE[hasPrivacyOf \rightarrow DRMControl] \\
 & \wedge ?per[hasPart \rightarrow ?prf]\wedge ?per[hasPart \rightarrow ?dif] \\
 & \wedge ?per[endowedWith \rightarrow ?ppr] \\
 & \wedge ?per[delegate \rightarrow IEEE] \\
 & \wedge Retain[hasDuration \rightarrow =2\#Month] \\
 & \wedge ?sdtme[hasPart \rightarrow ?dtme] \\
 & \wedge ?edtime[hasPart \rightarrow ?dtme]
 \end{aligned}$$

$$\begin{aligned}
 & \wedge subtract-dateTimes(?edtime ?sdtme) \leq Retain \\
 & \implies IEEE[endowedWith \rightarrow ?ppr] \wedge \\
 & ?ppr[appliedTo \rightarrow ?prf]\wedge ?ppr[appliedTo \rightarrow ?dit].
 \end{aligned}$$

In *policy(drm1-IEEE)* DRM policy, we use ODRL basic primitive vocabularies *principal*, *asset*, *right*, or *obligation* to define a license agreement terms between principals, e.g. library, registrar, university, and publisher. Similarly, in *policy(pp1-IEEE)* privacy declaration policy, we use P3P basic primitive vocabularies (*user*, *owner*, *purpose*, *right*, *condition*) to define terms of privacy declaration between data user and data owner. All of these basic primitive vocabularies are defined in the DRM or privacy protection ontology's schema, so the semantics of ODRL and P3P RELs are formalized (see Figure 3 and Figure 4).

2) *Policies declared in the NCCU library:* The NCCU library has two policies similar to those of the IEEE publisher: *policy(drm2-NCCULib)* for DRM access control and *policy(pp2-NCCULib)* for privacy policy declaration.

- *policy(drm2-NCCULib):*

policy as natural language:

If a student owns a valid student ID issued by department of registrar at the NCCU university, then a student is endowed with DRM usage rights {download, view, print} for all of the eJournal articles in a web server's of IEEE digital library through a web server of the NCCU library.

- *policy(pp2-NCCULib):*

policy as natural language:

If a person is endowed with DRM usage rights at a web server of the NCCU digital library and it has a purpose of enforcing DRM control on collecting, retaining, and disclosing client's data then the NCCU library is endowed with privacy usage rights {collect, retain, disclose} on a person's data, including profiles and digital traces in this web server under the condition of twelve months retention period since the data are first collected.

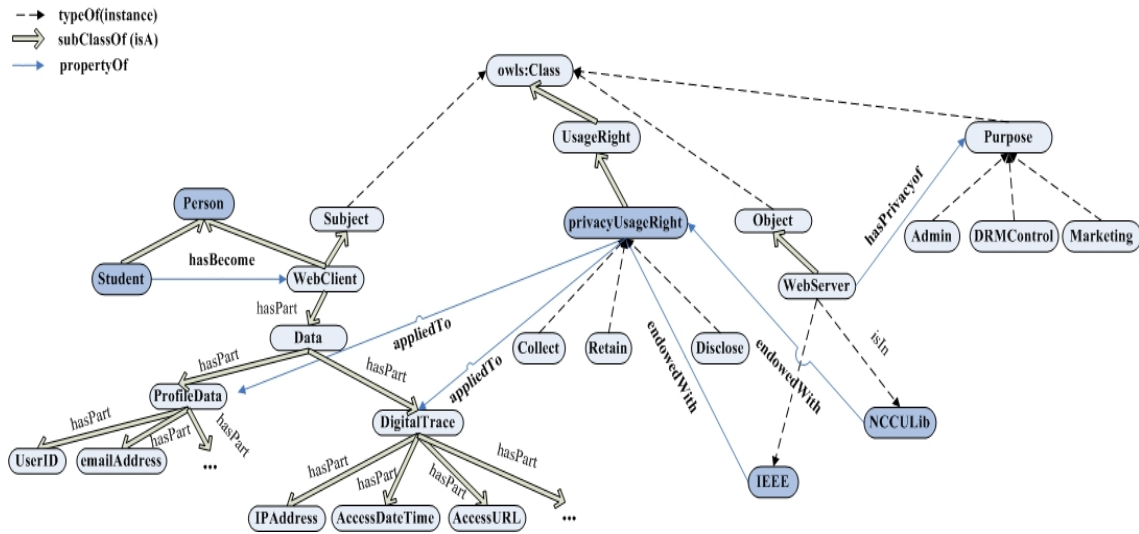


Fig. 3. PIF-based ontologies for privacy protection policies

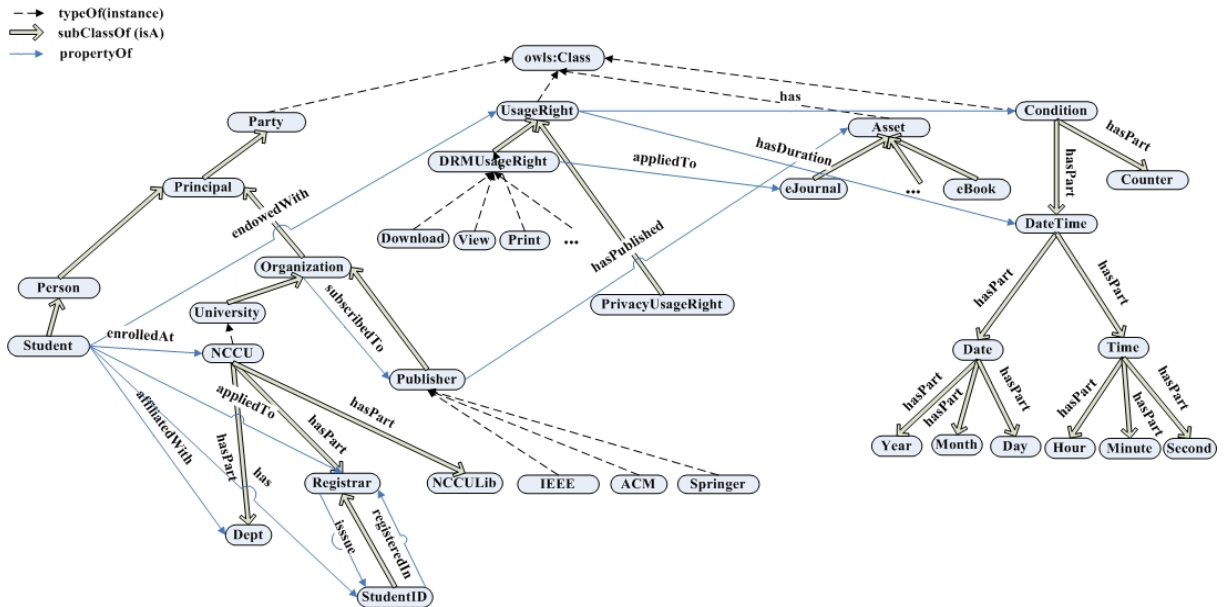


Fig. 4. PIF-based ontologies for DRM policies

B. Policies declared in a web client

A student of a web client *John* has three privacy protection policies, i.e., *policy(pp3-John)* to *policy(pp5-John)* to address how and what his personal data can (or cannot) be collected, retained, or disclosed from a web server:

- *policy(pp3-John)*:

policy as natural language:

If the NCCU digital library has a purpose of enforcing DRM control on collecting, retaining, and disclosing on the web client *John*'s data then it is endowed with privacy usage rights {collect, retain, disclose} on the web client *John*'s profiles and digital traces under the condition of retention period less than one hundred and twenty days since the data are first collected.

- *policy(pp4-John)*:

policy as natural language:

If a(n) {ACM, IEEE, Springer} *eJournal* distributor has a purpose of enforcing DRM control of collecting, retaining, and disclosing on the web client *John*'s data then it is endowed with privacy usage rights {collect, retain} on the web client *John*'s profiles under the condition of retention period less than thirty days since the profiles are first collected.

- *policy(pp5-John)*:

policy as natural language:

If the IEEE *eJournal* distributor has a purpose of enforcing DRM control of collecting, retaining, and disclosing on the web client *John*'s data then it is endowed with

privacy usage rights {collect,retain} on a web client John's digital traces under the condition of retention period less than fourteen days since the trace data are first collected.

C. A facilitator enables meta-PIF

For privacy protection policies *policy(pp1-IEEE)* to *policy(pp5-John)*, we use P3P basic primitive vocabularies to specify data *owner (or subject)*, data *user (or object)*, data *type, right, obligation* and *condition* as ontology's classes with associated properties to formalize the semantics of these vocabularies [9]. However, we also need to use Horn logic-based rules to express whether a web server is allowed to collect, retain, or disclose a particular client's profiles or digital traces under certain conditions, since a facilitator cannot use a DL-based ontology to decide whether a client has any particular access rights.

Policies are defined as a combination of ontologies and rules. In order to interchange and unify policies from a client and a server, we allow a facilitator to collect ontologies and rules within associated DRM and privacy protection's policies from them and to enable SemPIF policy's transformation and management services. The processes will be shown as follows:

1) **Ontologies mapping and aligning**

We have to map and align vocabularies from domain dependent ontologies of DRM and privacy protection policies. Thus, the example class vocabularies of "Student, Publisher" in *policy(drm1-IEEE)* and *policy(pp1-IEEE)* policies correspond to "WebClient, WebServer" class vocabularies in *policy(pp4-John)* to *policy(pp5-John)* policies. Furthermore, we need to align these ontology's schemata constructed with the above class and associated property vocabularies.

2) **Semantics mediating and unifying**

We need to mediate and unify the semantic differences between vocabularies and schema of ontologies belonging to different protection policies. For example, a condition of *Retain[hasDuration \rightarrow =2#Month]* in the *policy(pp1-IEEE)* corresponds to a condition of "retention period less than fourteen days" in the *policy(pp5-John)*. Even these vocabularies can be specified in XML-schema, but the semantic differences still need to be identified and aligned together through PIF-based policy transformation. The challenge is to understand the semantics of retention period shown in different privacy protection policies and to verify whether the conditions between these policies agree with each other.

3) **Resolving conflicts**

If possible, we have to resolve the conflicts between these policies. A facilitator initiates the reconciling processes between conflicting policies using the meta-PIF framework to exercise the policy management services. In this example, IEEE declares its intention to collect, retain, and disclose a web user's data in the *policy(pp1-IEEE)* policy for two months. The data include a web user's profiles and digital traces, which have been left on

a web server owned by IEEE. Web user John does not allow an IEEE web server to disclose his personal profile to the other partners. Thus, policies between *policy(pp1-IEEE)* and *policy(pp4-John)*, *policy(pp5-John)* are inconsistent in terms of privacy right and data retention period. To achieve policies reconciliation between client and server, we need to resolve the conflicts between these policies' conditions.

A facilitator uses meta-PIF-based policies to fix the policy conflicts that come from a client and a server. One approach is that a facilitator enables a policy priority-setting mechanism with meta-PIF-based policies to avoid the conflicts between a client and a server's policies. In this example, a facilitator might give a higher priority for a client's *policy(pp4-John)* and *policy(pp5-John)* than for a server's *policy(pp1-IEEE)* in the privacy protection domain. The defeasible logic of a meta-PIF's expression *Overrides(policy(?pid1),policy(?pid2))* for resolving conflicts of policies is a possible solution, where *policy(?pid1)* is bound to *policy(pp4-John)* and *policy(pp5-John)*; *policy(?pid2)* is bound to *policy(pp1-IEEE)*. Then, an IEEE web server's *policy(pp1-IEEE)* policy will be synchronized with the client's policies *policy(pp4-John)* and *policy(pp5-John)*.

Otherwise, a facilitator initiates a negotiation process between a client and a server to permit either side to modify its conflict conditions so that the conflicts can be diminished and finally removed. Based on the meta-PIF policies, a facilitator needs to acknowledge the client and the server before an ongoing reconciliation status can be achieved in each step of a negotiation process. This needs further study.

VI. CONCLUSION AND FUTURE PROSPECTS

We propose a semantics-enabled policy architecture SemPIF, which extends W3C's Semantic Web layered architecture. We have shown the SemPIF architecture to be a 4-layer framework, i.e., Unifying Logic (UNL), Policy Interchange Format (PIF), Privacy Protection and DRM (PPD), and Domain Specific Applications (DSA). A meta-PIF layer is also introduced, side by side with the corresponding PIF, allowing a facilitator to provide uniform services of interchange, reconciliation, and combination of multi-policies from various domains on the Web. A use case scenario of a facilitator employing SemPIF for multiple DRM and privacy protection policies on digital library subscription services is described to demonstrate the feasibility of this SemPIF architecture. The future prospects of this study are designing well-defined PIF and meta-PIF languages to enable a multiple web policies system implementation on the Web. Furthermore, we need to find a feasible combination of ontologies and rules to leverage the power of their knowledge representations for SemPIF.

ACKNOWLEDGEMENTS

This research was partially supported by the NSC Taiwan under Grant No. NSC 95-2221-E004-001-MY3, NSC 98-2918-E-004-003, and NSC 98-2221-E-004-009.

REFERENCES

- [1] S. Bechhofer et al., “OWL web ontology language reference”, Tech. Rep., W3C, Feb. 2004.
- [2] H. Boley et al., “Rule interchange on the web”, in *Reasoning Web 2007, Third International Summer School*, Dresden, Germany, sep. 2007, LNCS 4636, Springer.
- [3] L. Kagal et al., “Using semantic web technologies for policy management on the web”, in *21st National Conference on Artificial Intelligence (AAAI)*, July 2006, AAAI.
- [4] G. Tonti et al., “Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rei, and Ponder”, in *2nd International Semantic Web Conference (ISWC) 2003*, 2003, LNCS 2870, pp. 419–437.
- [5] P. Bonatti and D. Olmedilla, “Policy language specification, enforcement, and integration. project deliverable D2, working group I2”, Tech. Rep., REWERSE, 2005.
- [6] F. P. Patel-Schneider and I. Horrocks, “A comparison of two modelling paradigms in the semantic web”, *Journal of Web Semantics*, pp. 240–250, 2007.
- [7] H. Hilary Hosmer, “Metapolicies I”, *ACM SIGSAC Review*, vol. 10, no. 2-3, pp. 18–43, 1992.
- [8] Y. J. Hu, “Semantic-driven enforcement of rights delegation policies via the combination of rules and ontologies”, in *Workshop on Privacy Enforcement and Accountability with Semantics in conjunction with ISWC+ASWC’07*, 2007.
- [9] Y. J. Hu, H. Y. Guo, and G. D. Lin, “Semantic enforcement of privacy protection policies via the combination of ontologies and rules”, in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*, Taichung, Taiwan, June 2008.
- [10] de Jos Bruijn, “Rif rdf and owl compatibility”, Tech. Rep., W3C, Oct. 2009, <http://www.w3.org/TR/rif-rdf-owl/>.
- [11] Y. J. and Vicky Weissman Halpern, “A formal foundation for XrML”, *Journal of the ACM*, vol. 55, no. 1, pp. 1–42, 2008.
- [12] N. Li, T. Yu, and A. I. Antón, “A semantics-approach to privacy languages”, *Computer Systems and Engineering (CSSE)*, vol. 21, no. 5, Sep. 2006.
- [13] R. Pucella and V. Weissman, “A formal foundation for ODRL”, arXiv:cs/0601085v1, Cornell University, January 2006, <http://arxiv.org/abs/cs/0601085>.
- [14] I. Horrocks et al., “SWRL: A semantic web rule language combining OWL and RuleML”, 2004.
- [15] N. B. Grosz et al., “Description logic programs: Combining logic programs with description logic”, in *World Wide Web 2003*, Budapest, Hungary, 2003, pp. 48–65.
- [16] M. F. Donini et al., “AL-log: Integrating datalog and description logics”, *Journal of Intelligent Information Systems*, vol. 10, no. 3, pp. 227–252, 1998.
- [17] B. Motik, U. Sattler, and R. Studer, “Query answering for OWL-DL with rules”, in *3rd International Semantic Web Conference (ISWC) 2004*, 2004, LNCS 3298, pp. 549–563, Springer.
- [18] G. Karjoth and M. Schunter, “A privacy policy model for enterprises”, in *15th IEEE Computer Security Foundations Workshop (CSFW)*, June 2002, IEEE.
- [19] E. Rissanen, “eXtensible Access Control Markup Language (XACML) ver. 3.0”, May 2007.
- [20] A. H. Anderson, “A comparison of two privacy policy languages: EPAL and XACML”, in *Proceedings of the 3rd ACM Workshop on Secure Web Services (SWS’06)*, 2006, pp. 53–60, ACM.
- [21] L. Cranor et al., “The platform for privacy preferences (P3P) 1.0 (P3P 1.0) specification”, 2002, <http://www.w3.org/P3P/>.
- [22] Inc. ContentGuard, “XrML: The digital rights language for trusted content and services”, Tech. Rep., ContentGuard Inc., 2002.
- [23] S. Guth and R. Iannella, “Open Digital Rights Language (ODRL) version 2”, ODRL initiative working draft, The ODRL Initiative, February 2005.
- [24] E. J. Cohen, “DRM and privacy”, *Commun. ACM*, vol. 46, no. 4, pp. 47–49, 2003.
- [25] J. Feigenbaum et al., “Privacy engineering for digital rights management systems”, in *Digital Rights Management (DRM) 2001*, 2002, LNCS 2320, pp. 76–105, Springer.
- [26] D. J. Weitzner et al., “Creating a policy-aware web: Discretionary, rule-based access for the world wide web”, in *Web and Information Security*, E. Ferrari and B. Thuraisingham, Eds., pp. 1–31. Idea Group Inc., 2006.