Semantics-enabled Policies for Information Sharing and Protection in the Cloud

Yuh-Jong Hu, Win-Nan Wu, and Jiun-Jan Yang

Emerging Network Technology (ENT) Lab.
Department of Computer Science
National Chengchi University, Taipei, Taiwan
hu@cs.nccu.edu.tw,{99753505,98753036}@nccu.edu.tw
http://www.cs.nccu.edu.tw/~jong

Abstract. The cloud computing platform provides utility computing allowing people to have convenient and flexible information sharing services on the web. We investigate the inter-disciplinary area of information technology and law and use semantics-enabled policies for modeling legal regulations in the cloud. The semantics-enabled policies of information sharing and protection are represented as a combination of ontologies and rules to capture the concept of security and privacy laws. Ontologies are abstract knowledge representations of information sharing and protection which extracted manually from the data sharing and protection laws. Rules provide further enforcement power after ontologies have been constructed. The emerging challenges of legalizing semantics-enabled policies for laws in the cloud include mitigating the gap between semantics-enabled policy and laws to avoid any ambiguity in the policy representation, and resolving possible conflicts among policies when they are required to integrate the laws from multiple jurisdictions.

Keywords: semantics-enabled policies, information sharing, data protection, national security, cloud computing, privacy for social network cloud

1 Introduction

We are dealing with the problem of using information sharing services not only to enforce national security, but also to ensure information protection of personal privacy. Personal data on the social network, such as Facebook and Twitter, are usually collected, retained, processed, and retrieved across different jurisdictions in the cloud. The legal policy enforcement for cross-border information sharing and protection is much more difficult in the cloud than in a current computer environment. We show how national security and privacy laws can be modeled and enforced as semantics-enabled policies using ontologies and rules. These policies for modelling laws in reality can be mapped to the enforceable security policies in the cloud's data centers. In our formal policy framework, the semantics-enabled policies are integrated, managed, and enforced in order to provide the cross-border information sharing and protection services.

In the NIST's definition, cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. That can be rapidly provisioned and released with minimal management effort and service provider interaction. The cloud model is composed of five essential characteristics, e.g., on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service.

A new spectacular phenomenon of information sharing and service integration has been created on the social web 2.0 since cloud services, such as SaaS, PaaS, IaaS, were offered. Cross-border data integration in the cloud allows legal authorities to exploit the legitimate law enforcement processes to collect and use shareable personal information to counter international crimes. However, it is difficult to foresee the consequences that may arise in the enforcement of national security policies through cross-border information sharing on the social web without violating current privacy laws. Currently, the 'model contracts' and the 'Safe Harbor' program are used for cross-border information sharing for the transfer of personal data to third countries. Even though they are compliant with the EU Data Protection Directive (EC/95/46), they may not offer a workable solution to implement data sharing and protection services in the cloud [1].

1.1 Research Issues and Contributions

Research issues. We have identified several research issues on the semantics-enabled policy enforcement of information sharing and protection in the cloud: (i) policies are represented and interpreted without causing any ambiguity while enforcing them for services, (ii) to ensure that policies that are compliant with the laws, and information sharing and protection of legal concepts can be manually extracted from the laws in each judicial domain, (iii) to deploy and enforce the policies for national security and privacy protection purposes, where abstract semantics-enabled legal-aware policies are overlaid on the current OpenTC cloud infrastructure to activate the lower level security policies[1], (iv) to integrate and unify semantics-enabled policies from multi-domains in order to have cross-border data usage services, and (v) to enforce legalized policies when semantics-enabled policies are deployed in the formal policy platform.

Our contributions. Our main contributions are: (i) semantics-enabled policies are presented as a combination of ontologies and rules, and (ii) unifying privacy protection policies with national security policies in the social network cloud. For each information disclosure request, we intend to comply simultaneously with national security laws to counter-crimes and with privacy laws to protect civil rights. (iii) Automated policy integration is indicated as ontologies merging and rules integration from multi-domains. The high-level abstract semantics-enabled policies are mapped to national security and privacy protection policies. (iv) A data request for a counter-crime example is demonstrated to enforce national security. We intend to provide legal information sharing services without violating the data protection law for each jurisdiction.

[1] The EU FP6 Open Trusted Computing (OpenTC) project, http://www.opentc.net/

Outline. The remainder of the paper is organized as follows. In Section 2, we introduce background information and related work. The important design issues related to semantics-enabled formal policies, including policy representation, policy compliance, policy framework, and policy deployment are explained in Section 3. In Section 4, we discuss unifying policies through policy integration. We focus on an example for unifying privacy protection and national security policies and explicitly describe the policy enforcement of this example. In Section 5, we conclude this paper and point out possible future work.

2 Background and Related Work

Security and privacy are the two major challenges to deliver trusted information sharing and protection services in the cloud [2]. Given a particular cloud service infrastructure, we should allow only authorized users to use the services permitted by security and privacy laws. Once the services of information sharing cross-borders in the cloud, regulation compliance and enforcement become more difficult. This is because each domain is defined as an independent judicial area and only regulated by its own security and privacy protection laws. When information sharing crosses multi-domains, we have to integrate the laws from different jurisdictions to provide the intended services.

Sometimes resolving regulation conflicts between different judicial areas is unavoidable. To counter crimes, such as fraud or terrorism, we address the issue of possible cross-border information sharing on the social network in the cloud. Although a cloud infrastructure can provide much easier services of data sharing, a cloud provider must still respect the data protection laws from each legal domain to regulate its data collection, storage, and usage. We intend to apply the semantic web's ontology and rule technologies to represent the national security and privacy protection policies. The semantics-enabled policies are computable and machine understandable, so the legal compliant policies are enforced automatically by computer with little human intervention.

An enterprise server usually declares its privacy protection policies either in legal language for privacy statements or in computer privacy language for the Privacy Preference Platform (P3P) [3]. When a privacy language, such as P3P, is used for privacy statement declaration in a server, it always takes into account the Fair Information Principles (FIPs) extracted from the international privacy protection law, such as EU Data Protection Directive (EC/95/46). On the other hand, Enterprise Policy Authorization Language (EPAL) policies can be shown as access control policy (ACP) and data handling policy (DHP) [4].

ACP states the conditions that a requester must satisfy to gain access to a resource. DHP, on the other hand, indicates how the requester's information should be treated once it is revealed. In fact ACP and DHP are a data controller's promised policies created from unifying of the client's user privacy preferences and the server's privacy declarations [5] [6]. For each data request, an ACP is used for authenticating a legalized user to access the data. Then a DHP requests other servers' data usage, the same as an original data collector. But

P3P and EPAL privacy languages lack the formal and unambiguous semantics for a policy administrator to specify the privacy protection policies. The formal semantic policy resolves this problem by allowing a software agent to enforce various privacy protection policies automatically. In addition, ACP and DHP can be enhanced and used for information sharing and protection in the cloud.

One of the research challenges in solving the online privacy protection problem is to develop a privacy management framework using a formal semantics language thus empowering agents to enforce privacy protection policies. Agents also can detect and avoid any policy violations from each data request. We have established a semantic privacy protection model to address this issue [7]. We also intend to enhance the OpenTC's two-layered trusted virtual cloud infrastructure by using this semantic privacy protection model in the cloud [8]. A three-layered formal policy framework is presented to ensure the legal data sharing and to avoid the data protection laws violation in the social network cloud (see Figure 2). The purpose of information sharing is to permit legally collecting personal identification information (PII), such as email, online location, and phone numbers, in the social network cloud to counter-crimes.

We conclude that the dual objectives of greater national security and greater privacy protection can be achieved through unifying national security policies and data protection policies in the cloud. This statement is similar to the viewpoints suggested in [9]. In fact, the semantic web technologies were applied to a national security protection scenario to facilitate information sharing across intelligence community boundaries [10]. Another one, the Information-Sharing Agreement (ISAs) were constructed through agreed formal defined legal rules, derived from policies, to regulate and direct the inter-agency data flow [11].

3 Semantics-enabled Formal Policies

The well-known semantic web layered architecture[2] has undergone revisions reflecting the evolution of layers and their relationship. Semantics-enabled formal policies are formulated as ontology and rule knowledge bases with ontology and rule languages in the semantic web layered architecture. Many operations can be automated, thereby reducing ad-hoc program coding to a minimum, and enabling automated documentation [12].

An ontology is a formal, explicit specification of a shared conceptualization [13]. One key aspect of managing policies is the semantic heterogeneity and conflicts among policies. Using ontology as a formal representation of a policy and a meta-policy for solving the policy semantic heterogeneity and conflict are very promising. Furthermore rules empower the policy enforcement for information sharing and protection once the policy and meta-policy have been described as ontology.

[2] http://www.w3.org/2007/03/layerCake.svg

3.1 Formal Policy Representation

A formal policy is a declarative expression for a legal regulation that can be executed in a computer system without causing semantic ambiguity. A formal policy is created from a policy language, which is a combination of ontology language and rule language. Policy languages, such as Rein [14], KAoS [15], and Protune [12], have also been proposed – to allow agents to understand and enforce policies as intended by their semantics.

A formal policy is composed of ontologies and rules, where ontologies are created from an ontology language and rules are created from a rule language [16]. A formal protection policy aims at representing and enforcing data protection directives and national security principles, where the structures of privacy protection directives and national security principles are modeled as ontologies and the enforcement of these formal protection policies is shown as rules.

Using the policy ontology, a `Request` for data `hasCondition`, such as `DataUser`, `Purpose`, etc (see Figure 1). If multiple policies are applicable for a data request, we use `hasPriority` to set an execution priority. Otherwise, `Isolated Policy` `isBelongedTo` a `TLD` (Trusted Legal Domain). When a `Request` `getInTo` a `TLD` (see Section 3.3), the policies for this legal domain will be integrated. `DomainPolicy` is a meta-policy and it `hasTLD` to offer its `DataPolicy`.

A meta-policy is a policy about policies that provides a set of rules for realizing services needed for the management of policies [17]. A meta-policy consists of a set of rules for setting up the priority between privacy protection and national security polices. Policy management services are provided in a formal policy framework in Section 3.3. They could be implemented as meta-policies in Rein [14] or as policy administration tools in KAoS [15]. In Protune, the role of meta-policies is to govern policy behavior, to reduce ad-hoc programming efforts, and to improve policy readability and maintainability.

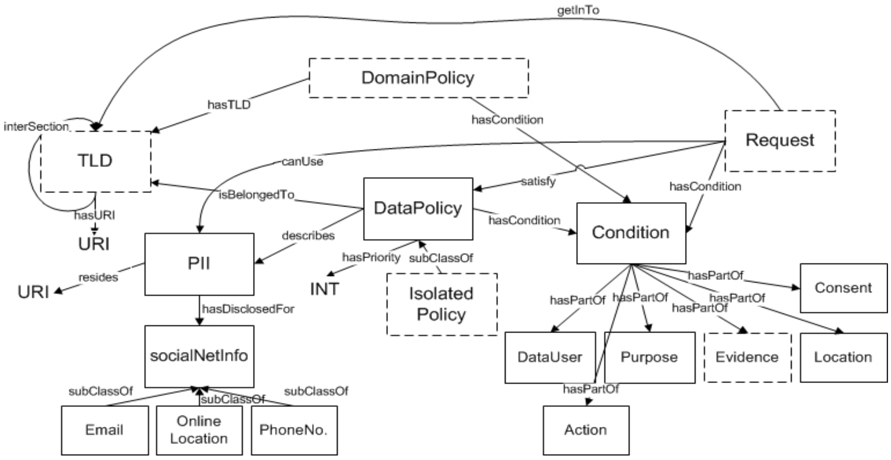

Fig. 1. A policy ontology is used for policy and data usage descriptions of a TLD.

3.2 Formal Policy Compliance

The cloud computing environment is an international global computer system infrastructure. Once dispersed, computer resources are installed and data is in the cloud, we face the challenges of providing legalized data sharing and protection services across jurisdictions. In the cloud, anyone can use anything from anywhere at anytime, so we must harmonize the laws that come from different jurisdictions. This also raises the regulation compliance issue where the formal policies enforced in the cloud must satisfy the data usage criteria indicated in the related laws.

Obviously current data protection and national security laws are not up-to-date on handling the cloud's cross-border data sharing and protection problems. We need to address research issues, not only for a law refinement, but also for a technology re-engineering. The ultimate objective of this study is to empower the use of flexible and agile cloud resources without violating the laws.

Semantics-enabled formal policies are inflexible if they are only compliant with current laws but do not comply with the new laws resulting from emerging information technologies. We propose a formal policy framework with flexible policy deployment, integration, and enforcement. In this framework, semantics-enabled data protection and national security policies are automatically unified to satisfy the purpose of national security enforcement through data sharing. However, we must also ensure that data protection laws are not violated. In this paper, a formal policy compliance of each data request is based on the *data usage context* of a user. It is a pre-condition in retrieving shared information that satisfies the laws. The laws that will be applied to a data request in a TLD depends on the data usage context of a data user. The legal boundary of a TLD is also based on the data usage context.

3.3 Formal Policy Framework

A trusted policy framework is essential to facilitate automatic policy integration and to meet the inter-domain's service-access requirements in the cloud [2]. We need a framework to guarantee that formal policies are compliant with the laws. In addition, they must be properly specified, verified, and enforced for any possible data access across domains.

Based on the trusted virtual domain's (TVD's) two-layered infrastructure [18], a semantics-enabled formal policy three-layered framework is presented (see Figure 2):

1. **Cloud Machine Domain (CMD)** layer
   A group of physical cloud computers with various virtual machines (VMs) are established within a trusted machine domain (TMD). A TMD allows a grouping of cloud computers connected by a VLAN switch to be protected as an isolated Intranet. Otherwise, a virtual privacy network (VPN) is set up to use a secure channel for TMDs and to provide secure data transmission between VMs.

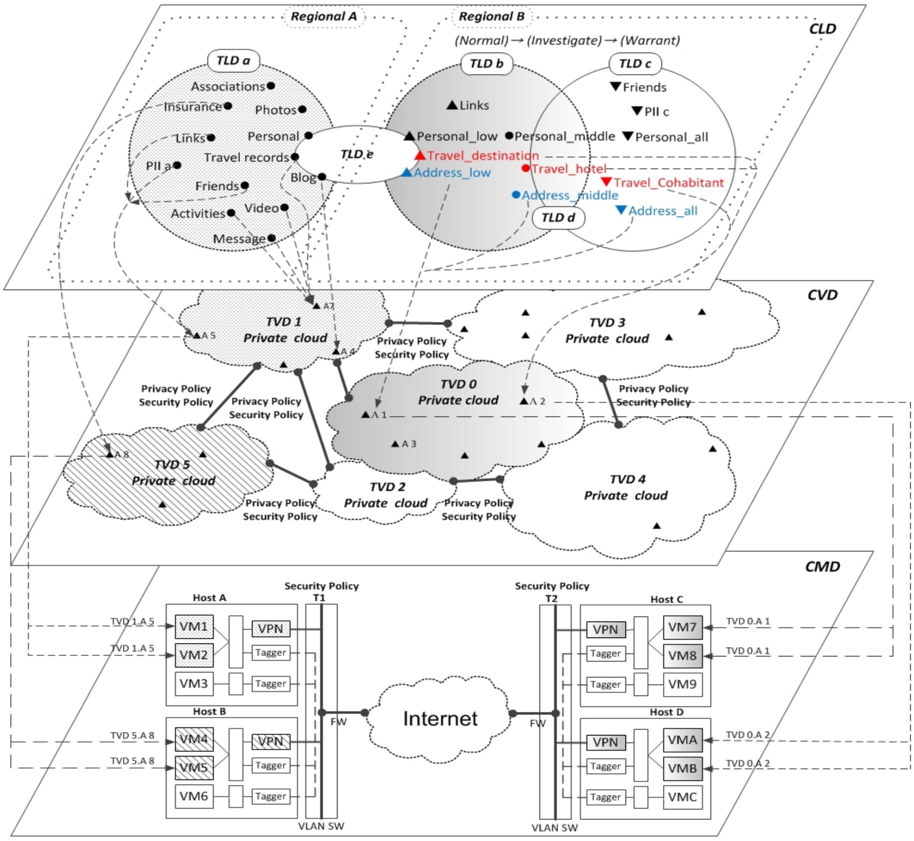

Fig. 2. A semantics-enabled formal policy framework with three policy domain layers: cloud machine domain (CMD), cloud virtual domain (CVD), and cloud legalized domain (CLD).

In the CMD layer, data centers are operated in the so-called *physical cages* model, wherein different customers' IT infrastructure runs on distinct physical resources. A physical boundary of a TMD depends on whether the hosts belongs to the same LAN within an Intranet. In the same LAN, hosts can communicate directly using the trusted physical link without traffic encryption.

2. **Cloud Virtual Domain (CVD)** layer

   Although a group of of VMs are dispersed across multiple physical cloud computers in TMDs, these VMs are still possibly configured into a virtual zone as a Trusted Virtual Domain (TVD) belongs to a specific customer in a private cloud. A TVD consists of a set of virtual machines, network configuration, storage and policies for access control and resource consumption. Protection policies are created for uniform secure services, such as storage, networking, and TVD membership in a TVD [8].

The CVD layer allows resource sharing among customers in the *logical cages* model. This enables a more flexible and efficient management of the data center's resources [8]. The logical boundary of a TVD is a secure logical domain, where security and storage usage policies are uniformly enforced within a TVD across its members.

3. **Cloud Legalized Domain (CLD)** layer
   Semantics-enabled policies are manually specified and are compliant with the current laws for data sharing and privacy protection in a Trusted Legal Domain (TLD). A TLD has a virtual legal boundary and use law compliant semantics-enabled policies to regulate data access. The semantics-enabled policies are translated into the network security and storage usage policies of a TVD.

   In the CLD layer, we use the *legal cages* model, compared with the *logical cages* model on the CVD layer, to provide uniformly legalized data sharing and protection services. A legal virtual boundary of a TLD defined for a person (or software) has limited data access rights to serve a purpose within a particular data usage context. For example, a national security law enforcer has the right to access any suspect's Facebook IP and email addresses from the list of friends' contacts whenever an investigation with certain evidence is allowed to do so. However, whether to grant or deny a data request permission still depends on an additional data usage context, such as where is the data requester's location, which data center is responsible for this data, and what applicable laws are used for this request, etc. Furthermore, the semantics-enabled policies can also define a permissible data flow between any two TLDs and regulate the flow under each TLD's law.

3.4 Formal Policy Deployment

Semantics-enabled policies are deployed in TLDs and enforced on the CLD layer in a formal policy framework. We aim to represent and enforce the high-level legal compliant semantics-enabled policies of TLDs. Thus the legal compliant policies of TLDs can be flexibly mapped into the security and privacy policies of TVDs. Consecutively, the security and privacy policies of TVDs are mapped into the security services of TMDs. The possible mappings from TLD(s) to TVD(s) are one-to-one, many-to-many that are similar to the mapping situations from TVD(s) to TVD data center(s) (or TVDc) implemented in the Xen Cloud Platform (XCP)[3] [8].

The legal virtual boundary of a TLD is determined by a particular law that regulates the data disclosure range and level, where the semantics-enabled policies are compliant with the law for this TLD. An intersection area is compliant with applicable laws from multiple TLDs. When a data usage context is initiated for a data user to request information, the possible semantics-enabled policies

[3] XCP http://www.xen.org/products/cloudxen.html.

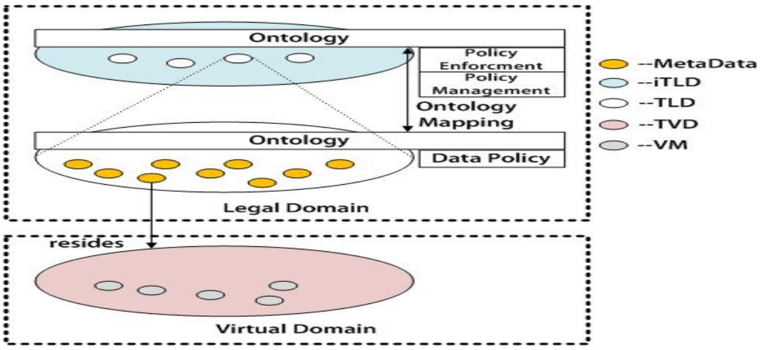

Fig. 3. A layer structure from legal domain to virtual domain, where the semantics-enabled policy is enforced and managed through meta-data, including domain-policy, meta-policy, to locate the real information.

related to the laws are executed. A data usage context includes a purpose, a data user's role, a requester location, a data location, and action, etc (see `Condition` in Figure 1).

In fact, this data usage context is based on the core definitions of data protection laws or national security laws. When a user submits a data request, a data usage context is created for this request with the policy enforcement ensuring that all of the information disclosure is legal under the laws. We face a law integration problem that turns into a formal policies integration problem.

In [8], two types of policy govern the cloud security in their TVDs. The first, security policy, limits the flow of networks and the usage of machine storage. The second, membership policy, defines which VM is allowed to join a TVD. Security policy is used for the security enforcement of TVDs on the CVD layer but the real policy enforcement mechanisms are still executed on the CMD layer. Semantics-enabled protection policies leverage the cloud security services of security policies because the CVD layer is unaware of the legal requirements.

4 Unifying Formal Policies

When a data user asks for information, a formal policy provides the concept of laws represented for a TLD with its possible enforcement constraints through a data usage context. Whenever a data usage context is suited to a multiple TLDs' intersection area, formal policies from these TLDs are unified to enforce data usage (see TLD d in Figure 2). In the procedure of unifying multiple formal policies, we map and merge local ontologies from policies and construct a global ontology of these unified formal policies [7]. For demonstration, two types of formal policies, privacy protection and national security, are unified to enforce a national security policy in the social network cloud (see Section 4.4).

4.1 Formal Policy Integration

People are getting aware of a more flexible and easier way to provide information sharing services in the cloud. For example, it is much easier to counter-terrorism through collecting a suspect's profile in the social network cloud. A challenge exists for how to achieve a privacy-preserving data integration and sharing services [19]. We attempt to apply the semantics-enabled formal policies integrated from various autonomous data sources in the cloud for information sharing once the laws are available. Information integration collects the data from autonomous and heterogeneous sources, and provides users with a unified view of these data through a so called global schema. The global schema, which is a reconciled view of the information, provides a single point of query services for end users. But the design of a data integration system includes several different issues, so it is very complex [20]. In this paper, we use a data integration service for information sharing in order to achieve a privacy-preserving data usage in the social network cloud.

4.2 Privacy Protection Policies

A privacy protection policy is a type of formal policy used for specifying a data usage constraint created by a data owner. After a policy is accepted, it represents a long-term promise made by an enterprise to its users. Therefore, it is undesirable to change an enterprise's promises to customers every time an internal access control rule changes. If possible, we should enable the P3P and EPAL policies to be accountable and transparent on information processing for a data owner to revise the data usage permissions in the future [3]. A data owner's PII is usually collected by a data controller, analyzed by a data processor, and accessed by a data user. All of these operations are protected under the privacy protection law's umbrella in a TLD b (see Figure 4). When a data request, including collection, analysis, and use, is asked for. We first consider the data usage context of this request. This allows us to decide how many and at what level PII can be disclosed in order to comply with the privacy laws.

4.3 National Security Policies

When a national security officer intends to access a group of suspects' PII, a data usage context is also created for this request. The data usage context of this information request includes a national security officer as a data user role, an investigation for homeland security as a purpose, the location of this data user, and the data itself. The policy ontology in Figure 1 details this concept description. Formal policies, based on the national security laws, are fetched to circumscribe the virtual boundary of a data usage in a TLD. Once the laws are revised, the data usage context will be changed and the virtual boundary of a data usage will be updated. Thus the formal policy framework in Figure 2 provides a flexible policy re-mapping while applying the new laws to redraw a TLD virtual boundary.

A PII is originally protected by the data protection law in the TLD b. When a data usage context is created to enforce the national security policy, a data usage is moved and circumscribed in the TLD d, and eventually migrated into the TLD c (see Figure 4). For a PII, if it sits in the TLD b but cannot move into the TLD d or TLD c with any data usage context, this implies that this PII cannot be disclosed through the national security policy enforcement.

4.4 Unifying Privacy Protection and National Security Policies

Some believe that the objectives of greater national security and greater personal privacy can be compromised but others disagree. For example, in [9] they believe that the ultimate solution balances the national security and privacy protection lies in utilizing information technologies for counter-terrorism and to safeguard civil liberties.

Pattern-based data queries face the challenge of privacy rights violation for false positives when identify the terrorist suspects. Therefore, pattern-based queries are required to issue iteratively in a privacy-sensitive manner. In this paper, the privacy violation issue can be avoided by using the right data usage context in a TLD. When we retrieve PII, the semantics-enabled polices reason. This provides additional evidence for updating the data usage context to allow enforcing national security policies iteratively; however, the information disclosure still respects the data protection policies.

When a data usage context is moved into the intersection of TLDs, i.e. TLD d, it implies that the privacy protection and national security policy are unified. Then a data usage request is regulated by these two type of policies. The ontologies of these policies will be mapped and merged. Rules will be further integrated to enforce the data usage within the conjunction, TLD d, of the multiple legal domains (see Figure 4). However, when applying pattern-based data usage in the conjunction area, we still have to follow the PII anonymous disclosure principles if supporting evidence is not strong enough to allow a full information disclosure. Handling anonymous information requires multiple stages of human-driven analysis with reasoning of unified policies. Therefore, national security analysts cannot act alone on the results of such queries until a third-party legal authority has established sufficient probable cause. Data analysts would refine queries in stages, seeking to gain more confirmation while involving privacy-protection techniques in the process [9].

Eventually, the data usage context will move to the TLD c, where it is beyond the TLD b's data protection boundary. Under that circumstance, the data usage context is only regulated and enforced by the national security laws. At this stage, data protection laws are out of context because national security officers have enough plausible evidence to prove that the suspects have committed a crime against the national security laws. Unifying privacy-protection policies with national security policies not only ensure privacy, but also encourages sharing data without fear of a privacy rights violation.

Sometimes, PII are collected and stored by a social network in multiple data centers dispersed across different judicial TLDs. Each TLD is an independent

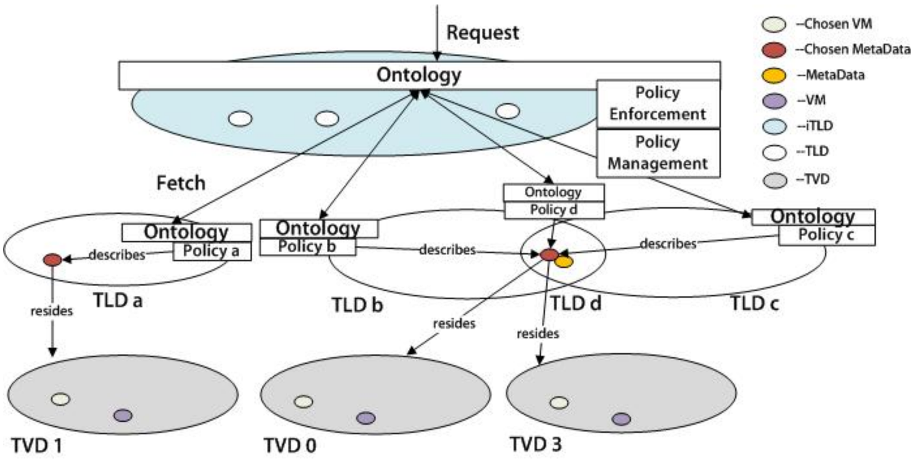

Fig. 4. A data usage context serves various information disclosure for TLDs.

legal domain and regulated by its own data protection and national security laws. Unless there is an establishment of (international) mutual agreements, a TLD's legal regulations do not allow its PII to be shared and transported to other TLDs. So the formal policies are only enforced locally without being unified with each other. Given this situation, the data usage and storing is restricted in a single legal domain, so the economic incentives of using a cloud's resources are hard to obtain.

4.5 Formal Policy Enforcement

Based on the policy ontology presented in Section 3.1, we reuse the vocabularies of this ontology to describe the concepts of domain-policy and data-policy for the policy enforcement rules in the TLD d. We demonstrate how to use the information sharing and privacy protection policies to serve the purposes of enforcing national security and privacy protection for a data request in the TLD d.

According to the policy ontology (see Figure 1), when a data request ?`x` with its data usage context ?`c` satisfy a `DomainPolicy`(?`d`)'s data usage context ?`dc`. A user is allowed to enter the TLD ?`tld` enforcing the investigation of national security(see rule (1)):

- A partial ontology for a domain policy:
  `hasTLD.DomainPolicy(d)`, `hasTLD`$^-$`.TLD(d)`.
  `hasCondition.DomainPolicy(d)`, `hasCondition`$^-$`.Condition(d)`.
  `hasPartOf.Condition(d)`, `hasPartOf`$^-$`.Purpose(investigation)`,
  `hasPartOf`$^-$`.DataUser(securityPersonnel)`,
  `hasPartOf`$^-$`.Location(TW)`, `hasPartOf`$^-$`.Evidence(things)`.
  `hasPartOf`$^-$`.Consent(nill)`.

- A rule for a domain policy enforcement:
  $\texttt{Request}(?\texttt{x}) \wedge \texttt{hasCondition}(?\texttt{x}, ?\texttt{c}) \wedge \texttt{Condition}(?\texttt{c}) \wedge \texttt{hasCondition}(?\texttt{d}, ?\texttt{dc})$
  $\wedge\ \texttt{Condition}(?\texttt{dc}) \wedge \texttt{DomainPolicy}(?\texttt{d}) \wedge \texttt{hasTLD}(?\texttt{d}, ?\texttt{tld})$
  $\longrightarrow \texttt{getInTo}(?\texttt{x}, ?\texttt{tld}) \leftarrow (1)$

  An ontology and a rule for a data policy $?\texttt{d}$ in the TLD $?\texttt{tld}$ allow a request $?\texttt{r}$ using PII $?\texttt{pii}$ of the social network information $?\texttt{sInfo}$ (see rule (2)) as follows:

- A partial ontology for a data policy:
  $\texttt{isBelongedTo}.\texttt{DataPolicy}(\texttt{d}),\ \texttt{isBelongedTo}^{-}.\texttt{TLD}(\texttt{d}).$
  $\texttt{describes}.\texttt{DataPolicy}(\texttt{d}),\ \texttt{describes}^{-}.\texttt{PII}(\texttt{d}).$
  $\texttt{hasDisclosedFor}.\texttt{PII}(\texttt{d}),\ \texttt{hasDisclosedFor}^{-}.\texttt{socialNetInfo}(\texttt{d}).$
  $\texttt{socialNetInfo}(\texttt{d}) \equiv \texttt{Email}(\texttt{d}) \sqcup \texttt{OnlineLocation}(\texttt{d}) \sqcup \texttt{phoneNo}.(\texttt{d}).$
- A rule for a data policy enforcement:
  $\texttt{Request}(?\texttt{r}) \wedge \texttt{satisfy}(?\texttt{r}, ?\texttt{x}) \wedge \texttt{DataPolicy}(?\texttt{d}) \wedge \texttt{describes}(?\texttt{d}, ?\texttt{pii})$
  $\wedge\ \texttt{hasDisclosedFor}(?\texttt{pii}, ?\texttt{sInfo}) \wedge \texttt{Evidence}(\texttt{things})$
  $\longrightarrow \texttt{canUse}(?\texttt{r}, ?\texttt{pii}) \wedge \texttt{socialNetInfo}(?\texttt{sInfo}) \leftarrow (2)$

5 Conclusion and Future Work

We present a three-layered formal policy framework to demonstrate how data usage crosses multiple judicial domains in the cloud. We focus on the design and modeling of the CLD layer with numerous TLD built-ins for the formal policy framework. In this innovative cloud framework, a TLD specifies its legal virtual boundary to accept a data request. When a data user asks for information disclosure using a role with a purpose from a location. A data usage context is created to determine which TLD with its various policies is eligible to constrain data usage. A domain-policy is applied to select which data policies are applicable for a real information disclosure within a TLD. A meta-policy is used for setting up the data-policy's priority for policy management when policy conflicts exist. Semantics-enabled policies are shown as a combination of ontologies and rules, where ontologies describe the concept of policies, including domain-policy, meta-policy and data-policy. Rules further enforce these different type of policies. The semantics-enabled policies are applied to a scenario where the national security policies for information sharing and the privacy protection policies for data usage are both satisfied. Finally, the CLD layer's proof-of-concepts prototype, based on the OpenTC architecture, has been implemented to justify our approach.

Acknowledgements

This research was partially supported by the NSC Taiwan under Grant No. NSC 99-2221-E-004-010 and NSC 100-2221-E-004-011-MY2.

References

1. Bruening, J.P., Treacy, B.C.: Cloud computing: privacy, security challenges. Privacy & Security Law Report (2009)
2. Takabi, H., et al.: Security and privacy challenges in cloud computing environments. IEEE Seurity & Privacy **8** (2010) 24–31
3. Antón, I.A., et al.: A roadmap for comprehensive online for privacy policy management. Comm. of the ACM **50** (2007) 109–116
4. Vimercati, S.D.C.d., et al.: Second research report on next generation policies, project deliverable D5.2.2. Technical report, PrimeLife (2010)
5. Ardagna, A.C., et al.: A privacy-aware access control system. Journal of Computer Security **16** (2008) 369–397
6. Karjoth, G., et al.: Translating privacy practices into privacy promises - how to promise what you can keep. In: POLICY'03, IEEE (2003)
7. Hu, Y.J., Yang, J.J.: A semantic privacy-preserving model for data sharing and integration. In: International Conference on Web Intelligence, Mining and Semantics (WIMS'11), Norway, ACM (2011)
8. Cabuk, S., et al.: Towards automated security policy enforcement in multi-tenant virtual data centers. Journal of Computer Security **18** (2010) 89–121
9. Popp, R., Poindexter, J.: Countering terrorism through information and privacy protection technologies. IEEE Seurity & Privacy **4** (2006) 24–33
10. Kettler, B., et al.: Facilitating information sharing across intelligence community boundaries using knowledge management and semantic web technologies. In Popp, L.R., Yen, J., eds.: Emergent Information Technologies and Enabling Policies for Counter-Terrorism. Wiley (2005) 175–195
11. Buchanan, W., et al.: Interagency data exchange protocols as computational data protection law. In: Legal Knowledge and Information Systems - JURIX, IOS Press (2010) 143–146
12. Bonatti, P., Olmedilla, D.: Policy language specification, enforcement, and integration. project deliverable D2, working group I2. Technical report, REWERSE (2005)
13. Gruber, T.R.: A translation approach to portable ontology specifications. Knowledge Acquisition **5** (1993)
14. Kagal, L., et al.: Using semantic web technologies for policy management on the web. In: 21st National Conference on Artificial Intelligence (AAAI), AAAI (2006)
15. Tonti, G., 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. LNCS 2870 (2003) 419–437
16. Hu, Y.J., Boley, H.: SemPIF: A semantic meta-policy interchange format for multiple web policies. In: 2010 IEEE/WIC/ACM Int. Conference on Web Intelligence and Intelligent Agent Technology, IEEE (2010) 302–307
17. Hosmer, H.H.: Metapolicies I. ACM SIGSAC Review **10** (1992) 18–43
18. Berger, S., et al.: Security for the cloud infrastructure: Trusted virtual data center implementation. IBM Journal of Research and Development (2009) 6:1–6:12
19. Clifton, C., et al.: Privacy-preserving data integration and sharing. In: Data Mining and Knowledge Discovery, ACM (2004) 19–26
20. Calvanese, D., Giacomo, G.D.: Data integration: A logic-based perspective. AI Magazine **26** (2005) 59–70