

Anlamsal Web’de Ontoloji Tabanlı Politikaların Kullanımı

Using Ontology Based Policies in Semantic Web

Özgü Can, Murat Osman Ünaler

Bilgisayar Mühendisliği Bölümü
Ege Üniversitesi

ozgu.can@ege.edu.tr , murat.osman.unalir@ege.edu.tr

Özet

Anlamsal Web, bilginin paylaşılmasını ve tekrar kullanımını sağlamak için, biçimsel anlambilimini kullanarak makinelerin diğer makineler ile haberleşmesine izin vermektedir. Ancak, bilginin paylaşılması gizlilik, erişim kontrolü, kimlik denetimi, yetki ve veri bütünlüğü gibi güvenlik ihtiyaçlarını getirmekte ve Anlamsal Web teknolojilerinin güvenliğini sağlayacak etkili mekanizmalara ihtiyaç duyulmaktadır. Anlamsal Web tabanlı politikalar bilgiye güvenli bir şekilde erişim için kullanılmaktadır. Politika, bir kaynak için o kaynakta herhangi bir değişiklik yapılmadan bir erişim kontrol mekanizmasının gerçekleştirilmesini sağlamaktadır. Ontoloji Tabanlı Erişim Kontrolü (OTEK) modelinde bilgiye erişim ontoloji tabanlı bir yaklaşım ile gerçekleştirilmektedir. Bu amaçla, erişim mekanizmaları ile ilgili bilginin modellenmesi için ontolojiler kullanılmaktadır. Sistemin daha iyi kişiselleştirme için kullanıcı ihtiyaçlarına yönelik olarak davranabilmesi amacıyla bu çalışmada etki alanı, profil ve tercih politikaları olmak üzere üç çeşit politika tanımlanmaktadır. Etki alanı ve profil politikaları kullanılarak kullanıcı tercihleri kısıtlanmakta, böylelikle de kullanıcının en iyi sorgu sonuçlarına ulaşması hedeflenmektedir.

Abstract

Semantic Web allows machines to share and reuse the information by using formal semantics for machines to communicate with other machines. However, sharing the information brings security needs like privacy, access control, authentication, authorization and data integrity, thus, efficient mechanisms are needed to provide the security of Semantic Web technologies. Semantic Web based policies are used to access data in a secure way. A policy provides an access control mechanism for a resource without making any change in the source. In Ontology Based Access Control (OBAC), accessing to data is achieved by an ontology based approach. For this purpose, ontologies are used to model data of access mechanisms. In this work, three kinds of policies are defined: domain, profile and preference policies allowing the system to behave according to the specific requirements of users for better personalization. User preferences are constrained by enforcing domain and profile policies, thus, users can achieve the best query results.

1. Giriş

Bugünkü webin içeriği makinelerden çok insanlar için biçimlendirilmiştir. World Wide Web’in (WWW) babası olan Time Berners Lee bugünkü web teknolojilerinin yetersizliklerini farkederek webi daha zeki bir hale getirmeye çalışmıştır. Bu amaçla makineler tarafından da anlaşılabilir web sayfalarına ve bilginin bütünleştirilmesi için ontolojilerin kullanımına ihtiyaç olduğu sonucuna ulaşmıştır. Böylelikle, Anlamsal Web kavramı ortaya çıkmıştır.

Anlamsal Web, bilginin paylaşılmasını ve tekrar kullanımını sağlamak için, biçimsel anlambilimini kullanarak makinelerin diğer makineler ile haberleşmesine izin vermektedir. Böylece, bugünkü webde kullanıcılar web sayfalarını okuyup kararlarını vermekteyken, Anlamsal Web’de ise ortak ontolojiler ve betimleme dilleri kullanılarak kullanıcıları temsil eden etmenler web sayfalarını okuyup anlayabilir ve karar verebilirler. Ontolojiler varlıklar için ortak tanımlamalardır. Farklı terimleri açıklamada ontolojilere ihtiyacı duyulduğundan web sayfalarının makineler tarafından anlaşılabilir olması için ontolojiler önemlidir.

Bilginin paylaşılması gizlilik, erişim kontrolü, kimlik denetimi, yetki ve veri bütünlüğü gibi güvenlik ihtiyaçlarını getirmekte ve Anlamsal Web teknolojilerinin güvenliğini sağlayacak etkili mekanizmalara ihtiyaç duyulmaktadır. Bu nedenle Anlamsal Web ile ilgili en temel çalışmalardan biri güvenilir Anlamsal Web’in geliştirilmesidir. Güvenilir Anlamsal Web ile güvenlik ihtiyaçlarının sağlanması amaçlanmaktadır. Şekil 1 Anlamsal Web için Tim Berners Lee tarafından geliştirilen katmanlı yapıyı göstermektedir, Şekil 2’de ise güvenli Anlamsal Web için her bir katmanda güvenliğin gerekli olduğu görülmektedir [1].

Veriye ve bilgiye erişimin kontrol edilmesi gerekmektedir. Güvenilir sistemlerde verilere erişimin kontrol edilmesi ve bilginin yönetilmesi sağlanmaktadır. Bu amaçla politikalar kullanılmaktadır. Politika, bir kaynak için o kaynakta herhangi bir değişiklik yapılmadan bir erişim kontrol mekanizmasının gerçekleştirilmesini sağlamaktadır. Erişim kontrol mekanizmalarında “Kullanıcı A, B1.doc dosyasını okuyabilir ve C1.doc dosyasına yazabilir.” gibi pozitif kurallar ve “Kullanıcı A, A1.doc dosyasına yazamaz ve D1.doc dosyasını okuyamaz.” gibi negatif kurallar tanımlanabilmektedir.

Mantık, Kanıt ve Güven
Kurallar/Sorgu
RDF, Ontolojiler
XML, XML Şemalar
URI, UNICODE

Şekil 1: Anlamsal Web Katmanlı Yapısı.

Güvenlik ile uyumlu Mantık, Kanıt ve Güven
Kurallar/Sorgu için Güvenlik
RDF, Ontolojiler için Güvenlik
XML, XML Şemalar için Güvenlik
URI, UNICODE için Güvenlik

Şekil 2: Güvenli Anlamsal Web için Katmanlar.

Anlamsal Web’de politika yönetimi bir kaynağa erişim için kuralların tanımlanması, kullanıcıların bu kuralları yorumlaması ve kurallara uyması için kullanılmaktadır. Anlamsal olarak zengin bir biçimde tanımlanmış olan politikalar, insan hatalarını ve politika çelişkilerini azaltmakta, politika analizini ve birlikte işlerliği kolaylaştırmaktadır [2].

Bu çalışmada Anlamsal Web politikalarının bilgiye güvenli bir şekilde erişim için nasıl kullanılacağına değinilecektir. Bu amaçla bilgiye erişimin ontoloji tabanlı bir yaklaşım ile gerçekleştirildiği Ontoloji Tabanlı Erişim Kontrolü (OTEK) modeli geliştirilmiştir. Bu modelde ontolojiler kullanılarak çeşitli politikaların yaratılması gerçekleştirilmektedir.

Dokümanın içeriği şu şekildedir: ikinci kısımda literatürde yer alan çalışmalara değinilmekte, üçüncü kısımda Ontoloji Tabanlı Erişim Kontrolü modeli açıklanmakta, dördüncü kısımda bir senaryo üzerinden yapılan çalışmalar anlatılmakta ve son olarak yapılacak çalışmalar özetlenmektedir.

2. İlgili Çalışmalar

Anlamsal Web teknolojilerine dayanan politika dilleri, politikaların heterojen etki alanı verileri üzerinde tanımlanmasına izin vermekte ve aynı bilgi modelini kullanmıyor olabilen katılımcılar arasında ortak anlamı desteklemektedir [3]. Son yıllarda yapılan erişim kontrol çalışmalarında iki paralel konu ele alınmaktadır [3]: gerçek dünya uygulama etki alanlarının politika ihtiyaçlarını karşılamaya yönelik erişim kontrol modellerinin geliştirilmesi ve erişim kontrolü için politika dillerinin geliştirilmesi. Bu iki paralel konunun, erişim kontrolü ve politika dilleri, güvenlik altyapısının gelişimini sağlamak için görevdeşlik yaratması gerektiği düşünülmektedir.

Anlamsal Web politika dillerinin bazıları şunlardır: Rei [2, 4], KAoS [2, 5], Ponder [2, 6], Rein [7], XACML [8], Proteus [9], Protune [10], APPEL [11], Trust-X [12], KeyNote [13], PeerTrust [14] ve WSPL [15]. Politikaların tanımlanması için

kullanılan en bilinen anlamsal web tabanlı iki politika dili Rei ve KAoS’tur.

KAoS politika dilinde ontolojiler OWL dili ile ifade edilmektedir. Web servisleri için politika ve etki alanı yönetimi servislerinden oluşmaktadır. KAoS Politika Ontolojisi (KPO) yetkiler (eyleme izin veren ya da yasaklayan kısıtlar) ve zorunluluklardan (bir durum meydana geldiğinde bazı eylemleri gerektiren ya da bu gereksinimden vazgeçilmesini belirten kısıtlar) oluşmaktadır [2]. KAoS, Sun’ın Java Etmen Servislerini (Java Agent Services - JAS) temel almaktadır ve muhakeme için JTP’yi (Java Theorem Prover) kullanmaktadır [5].

Rei, OWL-Lite temelli bir politika tanımlama dilidir. Kullanıcıların haklar, yasaklar, zorunluluklar ve özel izinler kavramlarını tanımlamasına izin vermektedir [2, 16]. Rei, politika geliştiricilerinin politikaları etki alanına özgü ontolojiler üzerinde RDF ve OWL gibi diller kullanılarak tanımlanmasına izin vermektedir. Sistemdeki haklar ve zorunlulukların varlıklar arasında değiş tokuş edilebilmesi için Rei politika dili konuşma edimleri kümesine sahiptir. Rei, politika tanımlamalarını muhakeme edebilmek için de bir Prolog politika motorunu kullanmaktadır. Rei politika motorunun tespit ettiği politika çelişkilerini çözmek için üstveri kullanılmaktadır. Politika motoru politika tanımlarını Rei ontolojisi ile tutarlı olacak şekilde hem Rei dilinde hem de RDF-S olarak kabul etmektedir [2]. KAoS ve Rei arasındaki temel fark, KAoS politika dili betimleme mantığını temel alırken Rei politika dilinin bilişimsel mantığı temel almasıdır.

Rol Tabanlı Erişim Kontrolü olan RBAC (Role Based Access Control) modelinde güvenlik politikası izinleri kullanıcıya değil rollere vermektedir. Kullanıcı, izinlerini sistemde tanımlı olan rollerine göre elde etmektedir. Böylece, kullanıcı rolleri ile ilişkili olan bütün izinlerini kalıt almaktadır ve bu rol hiyerarşisi ayrıca politikaların tanımlanmasını da basitleştirmektedir [17]. Örneğin, bir otel sisteminde, mevcut roller şu şekilde olabilir: yönetici, personel ve ziyaretçi. Eğer kullanıcı personel rolüne sahip ise kullanıcının otelin oda ile ilgili dosyalara erişim hakkı vardır, yönetici rolüne sahip olan kullanıcı ise hem otel oda dosyalarına hem de muhasebe ile ilgili dosyalara erişim hakkı vardır. Ancak, RBAC modelinde, kullanıcı-rol ve izin-rol atamaları için yönetimsel işlemlerin gerekli olması, roller ve izinlerin sayısındaki üstel artışın kullanıcı-rol ve izin-rol atama işlemlerini masraflı bir hale getirmesi gibi bazı sınırlamalar bulunmaktadır [18]. RBAC modelinde yer alan bu sınırlamalar nedeni ile bu çalışmada profil tabanlı politika yaklaşımı kullanılmaktadır.

3. Ontoloji Tabanlı Erişim Kontrolü

Politikalar günlük hayatımızda bir çok alanda karşılaştığımız bir kavramdır. Erişim kontrolü, eğitim, hükümet ve sağlık politikaları gibi çeşitli politika kavramları bulunmaktadır. Politika sistemin davranış şeklini belirten bir durumdur. Bir karar verme süreci olan politika, hem bir karar destek sistemi hem de bildirimsel deyim davranış sistemi olarak davranmaktadır [1].

Anlamsal Web’de politikaların tanımlanması için ontoloji dillerinden yararlanılmaktadır. Thomas R. Gruber tarafından yapılmış olan, daha sonrada Rudi Studer tarafından yenilenmiş olan tanımda ontoloji kavramsallaştırmanın açık

ve biçimsel bir belirtimdir [19]. Bilginin temsilinde ontolojiler kullanılmaktadır. Ontolojiler nesnelere, kavramlar ve ilişkiler tanımlayarak belirli bir etki alanına ait bilginin modellenmesini sağlamaktadırlar. Böylece sistemler arasında verilerin değiş tokuşu için standart kavramsal söz varlıkları belirtilmekte, bilgi tekrar kullanılabilir, sorgulamaların cevaplanması için servisler sağlanmakta ve heterojen sistemler arasında birlikte işlerliği kolaylaştıran servisler sunulmaktadır.

Bu çalışmada, erişim mekanizmaları ile ilgili bilginin modellenmesi için ontolojiler kullanılmaktadır. Oluşturulan bu yapı Ontoloji Tabanlı Erişim Kontrolü (OTEK) modeli olarak tanımlanmaktadır. OTEK'te; erişilecek nesne, bu nesne üzerinde gerçekleştirilebilecek eylemler ve bu eylemlerin hangi şartlar altında gerçekleştirilebileceğini belirten kısıtlar ontolojik olarak tanımlanmaktadır. Böylelikle, anlamsal olarak bütünlüğü olan parçaların yönetilmesi sağlanmaktadır. İkinci kısımda bahsedilen RBAC modelinde erişilecek kaynak ile ilgili olarak herhangi bir üst veri bilgisi bulunmamaktadır. OTEK modelinde ise erişilecek kaynak ve bu kaynağa erişilecek varlık ile ilgili üst bilgiler oluşturulmakta, politikalar da bu üst veriler temel alınarak yaratılmaktadır.

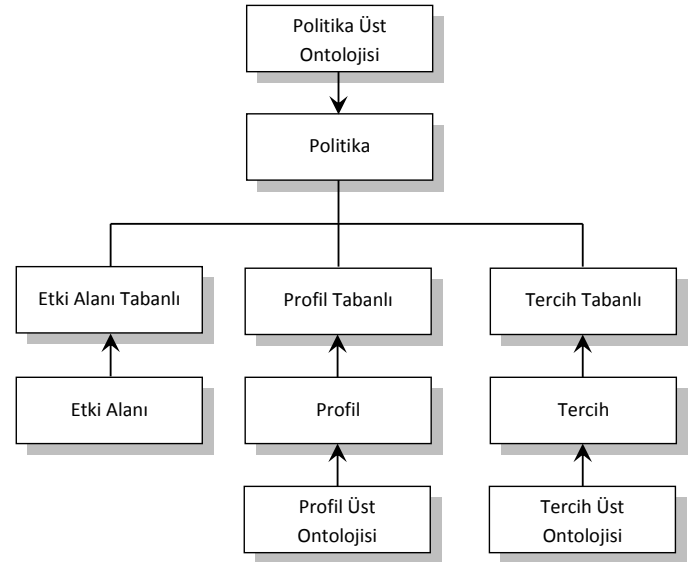
OTEK modelinde politika nesnelere olarak izin, yasak, zorunluluk ve özel izin tanımlanmaktadır. İzin, veriye ya da servise erişimin neleri yapabileceğini; yasak, neleri yapamayacağını; zorunluluk, neleri yapması gerektiğini; özel izin ise neleri yapmasına gerek kalmadığını belirten durumdur.

Anlamsal Web teknolojilerine dayanan politika dilleri, politikaların heterojen etki alanı verileri üzerinde tanımlanmasına izin vermekte ve aynı bilgi modelini kullanmıyor olabilen katılımcılar arasında ortak anlamı desteklemektedir [3]. Bu çalışmada, farklı profiller ve bir profilin çeşitli tercihleri heterojen etki alanı verilerini oluşturmaktadır. Profillerini oluşturan ve güncelleyen kullanıcılar sistemin katılımcılarını oluşturmaktadır.

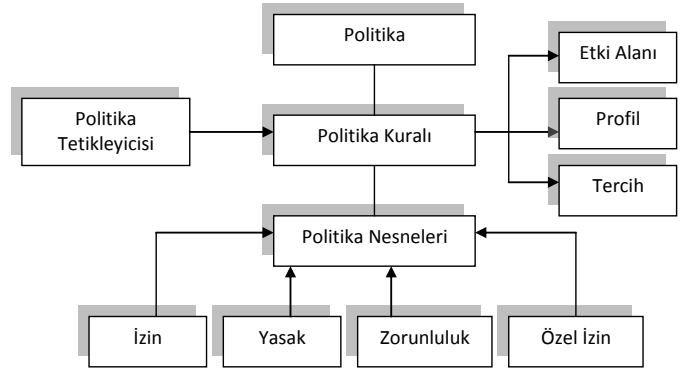
Sistemin daha iyi bir kişiselleştirme için kullanıcı ihtiyaçlarına yönelik olarak davranabilmesi amacıyla etki alanı, profil ve tercih politikaları olmak üzere üç çeşit politika tanımlanmaktadır. Şekil 3 tanımlanan politika ontolojilerini göstermektedir.

Bu çalışma kapsamında yer alan politika kavramı ve politika elemanları arasındaki ilişkiler Şekil 4'te yer almaktadır. Politika kurallarının kimlere uygulanacağını ve hangi durumlarda politikaların tetikleneceğini belirtmesi gerekmektedir. Bu çalışmada; etki alanı, profiller ve bu profillerin tercihleri üzerine politika kuralları tanımlanmaktadır.

Etki alanı ve profil politikaları kullanılarak kullanıcı tercihleri kısıtlanmaktadır. Kullanıcı, tercihlerini mümkün olabilecek seçenekler arasından yapmaktadır. Böylelikle, tercihler kısıtlandırılarak en iyi sorgu sonuçlarına ulaşılabilecektir. Örneğin, eğer bir turist evcil hayvanlara izin verilen bir odada kalmak istiyorsa, otel politikasının yürütülmesinden sonra kullanıcıya evcil hayvanlara izin verilen otellerin isimleri listelenecektir. Politika ve tercih arasındaki ontolojik ilişkinin sağlanabilmesi için politika eylemleri tercihleri temel almaktadır.



Şekil 3: Politika Ontolojileri.



Şekil 4: Politika ve Politika Elemanları.

4. Senaryo

Bu kısımda, kullanılan senaryo açıklanacaktır. 4P Yazılım Şirketi yıllık şirket toplantısını Paris'te Hilton Paris otelinde gerçekleştirmektedir. Yazılım geliştiriciler, yöneticiler ve ortaklar bu toplantıya katılabilmektedir. Cem yazılım geliştirici, Can ise yazılım geliştirme takımının müdürüdür. Can Paris'e eşi Selin ile gitmeyi planlamaktadır. Ali ise 4P şirketinin ortak şirketlerinden birisini temsil etmektedir.

4P şirketinin otel ile yaptığı anlaşmaya göre şirket çalışanları otelin bütün imkanlarından yararlanabilmektedir. Şirket çalışanlarının otelin açık büfe ve buhar banyosu gibi ekstra hizmetleri için herhangi bir ödeme yapmalarına gerek yoktur. Ancak oda manzarası seçiminde otelin diğer ziyaretçileri istedikleri oda manzarasını seçebilirken 4P şirketi çalışanları oda manzarası seçiminde Eiffel manzaralı odaları seçememektedir. Ayrıca, Hilton Paris otelinin bütün ziyaretçileri otelin kablosuz internet erişiminden faydalanabilmektedir. Otelin bir diğer kuralı da oda-kahvaltı seçimi yapmış olan ziyaretçilerin açık büfeden yararlanamayacağıdır.

Bu çalışmada yer alan ontolojiler OWL¹ ontoloji dili ile Protégé² ontoloji editörü kullanılarak yaratılmaktadır. Ontolojilerin saklanması ve ontolojilere erişilebilmesi için SESAME³ veri deposu kullanılmaktadır. Ontolojilerin ayrıştırılması ve modelinin oluşturulabilmesi için Jena⁴ kullanılmaktadır. Jena, Anlamsal Web uygulamalarının geliştirilmesi için kullanılan bir Java çerçevesidir. Jena, çıkarsama işlemlerini gerçekleştirebilmek için bir çıkarsama motorunu içermektedir.

4.1. Etki Alanı Politika Ontolojisi

Etki alanı politikalarında, politikalar ilgili etki alanı kurallarına göre oluşturulmaktadır. Senaryo kapsamında ele alınan turizm etki alanı ontolojisi temel alınarak HotelPolicy politikası oluşturulmuştur. Otel ile ilgili oluşturulan politikaların bir kısmı şu şekildedir:

Hilton Paris otelinde odalarda sigara içmeye izin verilmemektedir. (Yasak)

```
Accommodation(HiltonParis)\hasRoom(HiltonParis, Guestroom)
  A smokingAllowed(Guestroom, false)
  → Prohibition(Smoking, HiltonParis)
```

Turizm etki alanı ontolojisi olarak DERI tarafından geliştirilen e-tourism⁵ ontolojisi temel alınmıştır. Geliştirilen senaryo kapsamında bu etki alanı ontolojisine çeşitli eklemeler yapılarak genişletilmiştir. Genişletilmiş turizm ontolojisi bağlantısı Ek kısmında yer almaktadır.

4.2. Profil Tabanlı Politika Ontolojisi

Politika, kullanıcı profil bilgisini kullanarak kullanıcının ideal davranışlarını belirlemektedir. Profillemeye aynı sınıftaki kullanıcıların kümesinin oluşturulmasıdır. Profiller bilginin belirli bir kullanıcıya uyarlanmasına yardımcı olmaktadır [20]. Kullanıcılar yaş ve meslek gibi ortak özellikler ya da kullanıcıların yapmış oldukları ortak ilgileri dikkate alınarak gruplandırılmaktadır. Örneğin, yaşı 18 ve 35 arasında olan kullanıcılar "Genç" profiline, Profesör olarak çalışan kullanıcılar "Akademik" profiline sahip olmaktadır. Roller kullanıcılar olmadan da yaratılabilirken, profiller kullanıcılar olmadan yaratılamamaktadır. Profillemeye, kullanıcı olmadan profil olmamaktadır. Bu nedenle profillemeye kullanıcı bilgisine ihtiyaç duyulmaktadır. Ancak, rollerin kullanılması durumunda herhangi bir kullanıcı bilgisine ihtiyaç duyulmamaktadır. RBAC modelinde yer alan sınırlamalar nedeni ile bu çalışmada roller yerine profiller kullanılmaktadır. Profil tabanlı politikalar oluşturulurken profil üst ontolojisi⁶ kullanılarak yaratılmış olan profiller temel alınmaktadır. Örnek bir etki alanı politika kuralı şu şekildedir:

Turist profili Eiffel manzaralı odada kalabilir. (İzin)

```
Profile(Tourist)\hasView(Guestroom, Eiffel)
  → Permission(StayIn, Guestroom)
```

¹ Web Ontology Language, <http://www.w3.org/TR/owl-features>.

² Protégé ontoloji editörü, <http://protege.stanford.edu>.

³ Sesame veri deposu, <http://www.openrdf.org>.

⁴ Jena Anlamsal Web Çatısı, <http://jena.sourceforge.net>.

⁵ <http://e-tourism.deri.at/ont/e-tourism.owl>

⁶ Profil üst ve profil ontolojileri olarak yüksek lisans öğrencisi Okan Bursa tarafından geliştirilen ontolojiler kullanılmıştır.

4.3. Tercih Tabanlı Politika Ontolojisi

Tercihler, tercih yapan varlıkları kümelemektedir. Politikalar bu tercihlerin yönetilmesi için kullanılmaktadır. OTEK modelinde, tercih tabanlı politikaların temel aldığı tercihler, tercih üst ontolojisi kullanılarak oluşturulmaktadır. Tercih politikası, ilgili etki alanında aynı tercihlere sahip olan kullanıcılar için kurallar tanımlamaktadır. Bu çalışmada, bu kullanıcılar anonim profili olarak kabul edilmektedir. Örneğin;

Oda-kahvaltı tercihi yapan kişiler açık büfeden yararlanamaz. (İzin)

```
Profile(Anonymous)\hasPreference(bedBreakfast, true)
  → Prohibition(Use, SnackBar)
```

Tercih tabanlı politika ontolojisinde eylemlerin kısıtlamaları belirtilirken tercih üst ontolojilerinde⁷ tanımlanmış olan değerler kullanılmaktadır. Üst tercih ontolojilerinin bağlantıları Ek kısmında verilmiştir.

5. Sonuçlar

Bu çalışmada, Anlamsal Web teknolojilerinde güvenliğin sağlanması ve kişiselleştirmenin gerçekleştirilip kullanıcı ihtiyaçlarına yönelik sorgulamalardan etkili sonuçlar elde edilebilmesi için Anlamsal Web teknolojilerine dayanan politikalar kullanılmaktadır.

Politikalar tercih çelişkilerinin çözülmesi için de kullanılacaktır. Eğer kullanıcı tercihlerinde bir çelişki meydana gelirse son karar politika tarafından verilecektir. Örneğin, "Konferans katılımcıları dağ manzaralı odalarda kalabilirler." şeklindeki bir otel politika kuralına karşılık kullanıcının yapmış olduğu oda manzarası tercihi "deniz manzaralı" ise bu durumda bir çelişki meydana gelmiş olacaktır. Kullanıcı profili turist ya da konferans katılımcısı şeklinde olabilir. Eğer kullanıcı konferans katılımcısı profilinde işlem yaparsa son karar bir yasak şeklinde olacak, ancak eğer turist profilinde işlem yaparsa oda manzarası tercihinde herhangi bir kısıtlama ile karşılaşmayacaktır. Politika, çelişkileri öncelikler ve üstünlükler ilişkilerini belirterek çözmektedir [16].

Gelecek çalışmalarda, politika çelişkilerinin çözülmesini içeren politika ontolojileri OTEK modeline dahil edilecektir. Ayrıca, senaryo kapsamında çeşitli sorgular gerçekleştirilecektir. Bu amaçla, SESAME veri deposunun SPARQL⁸ sorgu modülü kullanılacaktır. Bu çalışmalara paralel olarak, kullanıcı arayüzünün ve politika çıkarsama motorunun geliştirilerek OTEK modelinin kodlanması ile ilgili çalışmalar Jena API kullanılarak NetBeans⁹ ortamında yürütülecektir.

6. Kaynaklar

- [1] Thuraisingham, B., *Building Trustworthy Semantic Webs*, Auerbach Publications, ISBN:0849350808, 2007.
- [2] Tonti, G., Bradshaw, J. M., Jeffers, R., Monranari, R., Suri, N., Uszok, A., "Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KaoS, Rei, and Ponder", *2nd International Semantic Web*

⁷ Tercih üst ontolojileri doktora öğrencisi Dilek Tapucu tarafından geliştirilmiştir.

⁸ SPARQL, <http://www.w3.org/TR/rdf-sparql-query>.

⁹ NetBeans IDE, <http://www.netbeans.org>.

- Conference (ISWC 2003), 2003, 419-437.
- [3] Finin, T. et al., "ROWLBAC - Representing Role Based Access Control in OWL", *Proceedings of the 13th Symposium on Access Control Models and Technologies*, 2008.
- [4] Kagal, L., Finin, T., Joshi, A., "A Policy Language for a Pervasive Computing Environment", *POLICY '03: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*, 2003, 63.
- [5] Uszok, A., Bradshaw, J. M., Jeffers, R., "KAoS: A Policy and Domain Services Framework for Grid Computing and Semantic Web Services", *Second International Conference on Trust Management*, 2004.
- [6] "Ponder: A Policy Language for Distributed Systems Management", <http://www-dse.doc.ic.ac.uk/Research/policies/ponder.shtml>.
- [7] "Rein Policy Framework for the Semantic Web", <http://groups.csail.mit.edu/dig/2005/05/rein/>.
- [8] "XACML: OASIS eXtensible Access Control Markup Language", http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.
- [9] Toninelli, A., Montanari, R., Kagal, L., Lassila, O., "Proteus: A Semantic Context-Aware Adaptive Policy Model", *POLICY 2007: 2007 IEEE Workshop on Policies for Distributed Systems and Networks*, 2007, 129-140.
- [10] Bonatti, P., Olmedilla, D., "Policy language specification", *Project Deliverable D2*, Working Group I2, EU NoE REVERSE, 2005.
- [11] Cranor, L., Langheinrich, M., Marchiori, M., Presler Marshall, M., Reagle, J., "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification", *W3C Recommendation*, <http://www.w3.org/tr/p3p>, 2002.
- [12] Bertino, E., Ferrari, E., Squicciarini, A. C., "Trust-X: A Peer-to-Peer Framework for Trust Establishment", *IEEE Transactions on Knowledge and Data Management*, 16(7), 2004, 827-842.
- [13] Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A., "The KeyNote Trust-Management System Version 2", *RFC 2704 (Informational)*, 1999.
- [14] "PeerTrust", <http://www.l3s.de/peertrust>.
- [15] Anderson, A. H., "An Introduction to the Web Services Policy Language (WSPL)", *Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04)*, 2004, 189.
- [16] Kagal, L., Finin, T., Joshi, A., "A Policy Based Approach to Security for the Semantic Web", *2nd International Semantic Web Conference (ISWC 2003)*, 2003, 402-418.
- [17] Cuppens, F., Miège, A., "Modelling Contexts in the OrBAC Model", *19th Annual Computer Security Applications Conference*, 2003.
- [18] Yuan, E., Tong, J., "Attributed Based Access Control (ABAC) for Web Services", *In ICWS'05: IEEE International Conference on Web Services*, 2005, 569.
- [19] Gruber, T.R., "Toward principles for the Design of Ontologies Used for Knowledge Sharing", *International Journal of Human-Computer Studies*, Volume 43 , Issue 5-6, 1993, 907-928.
- [20] Dzbor, M., Motta, E., "Engineering and Customizing Ontologies", *Ontology Management, Semantic Web, Semantic Web Services, and Business Applications*, 2008, 25-57.

İlgili ontolojiler aşağıdaki bağlantılarda bulunabilir.

Rei Politika Üst Ontolojileri

<http://www.cs.umbc.edu/~lkagal1/rei/ontologies/ReiAction.owl>
<http://www.cs.umbc.edu/~lkagal1/rei/ontologies/ReiAnalysis.owl>
<http://www.cs.umbc.edu/~lkagal1/rei/ontologies/ReiConstraint.owl>
<http://www.cs.umbc.edu/~lkagal1/rei/ontologies/ReiDeontic.owl>
<http://www.cs.umbc.edu/~lkagal1/rei/ontologies/ReiEntity.owl>
<http://www.cs.umbc.edu/~lkagal1/rei/ontologies/ReiMetaPolicy.owl>
<http://www.cs.umbc.edu/~lkagal1/rei/ontologies/ReiPolicy.owl>

Politika Ontolojileri

<http://efe.ege.edu.tr/~ozgucan/dr/Policy/HotelPolicy.owl>
<http://efe.ege.edu.tr/~ozgucan/dr/Policy/ProfilePolicy.owl>
<http://efe.ege.edu.tr/~ozgucan/dr/Policy/PreferencePolicy.owl>

Profil Üst Ontolojisi

<http://efe.ege.edu.tr/~odo/Ontology/MetaProfile.owl>

Profil Ontolojisi

<http://efe.ege.edu.tr/~odo/Ontology/Profile.owl>

Tercih Üst Ontolojileri

<http://efe.ege.edu.tr/~odo/Ontology/PMO.owl>
<http://efe.ege.edu.tr/~odo/Ontology/PVD.owl>

Etki Alan Ontolojisi

http://efe.ege.edu.tr/~ozgucan/dr/Ontology/I_Tour_mdfy.owl