TÜRK BİLİM ARAŞTIRMA VAKFI
TÜBAV
1995
TURKISH SCIENCE-RESEARCH FOUNDATION
TUBAV BILIM DERGISI

Yıl: 2010, Cilt:3, Sayı:3, Sayfa:238-249

ONTOLOJİ TABANLI BİLGİ SİSTEMLERİNDE ERİŞİM DENETİMİ: ULUSAL AŞI BİLGİ SİSTEMİ İÇİN DURUM ÇALIŞMASI

Murat Osman Ünalır[1*], Özgü Can[1], Emine Ünalır[1]

[1]Ege Üniversitesi Bilgisayar Mühendisliği Bölümü, Bornova-İzmir, Türkiye

Özet

Günümüzdeki webin sunduğu verinin, sadece insanlar değil makineler tarafından da aynı şekilde anlaşılarak, sistemler ve kullanıcılar arasında bilgi paylaşımını ve birlikte çalışabilirliği sağlamak, Anlamsal Web'in ulaşmak istediği hedefler arasında yer almaktadır. Özellikle, verinin anlamsal tanımının verildiği ontolojilerin üzerinden çıkarsama yapılmasını destekleyen alana özgü ontoloji tabanlı bilgi sistemleri geliştirilmeye başlanmıştır. Oldukça çok sayıda insan ve makine kullanıcısı olan bu sistemlerde bilgi paylaşımı desteklenirken, erişim denetiminin sağlanması ve olası çelişkilerinin çözümlenmesi gerekmektedir. Bu çalışmada ontoloji tabanlı bilgi sistemlerinde erişim denetiminin sağlanması ve çelişkilerin çözümlenmesi için Ontoloji Tabanlı Erişim Denetim (OBAC) modelinin sunduğu çözümler anlatılmaktadır. Mevcut erişim denetim uygulamalarında Rol Tabanlı Erişim Denetimi (RBAC) kullanılmaktadır. OBAC, RBAC'in getirdiği yönetimsel ek yükler nedeni ile rol tabanlı erişim denetimi kullanan uygulamalardan farklı olarak, profil tabanlı bir erişim denetimi sunmaktadır. Bu amaçla, kişiye özel bilgi anlamsal olarak modellenmekte ve erişim denetiminin bir parçası haline getirilmektedir. Bu çalışmada, sağlık alanındaki aşı ve aşı uygulamalarına ilişkin bilgi ve hizmetlerin sunulması hedeflenerek, ontoloji tabanlı bilgi sistemi olarak geliştirilmekte olan Ulusal Aşı Bilgi Sistemi'ndeki (UABS) erişim denetim desteği, OBAC'in kullanıldığı bir durum çalışması ile verilmektedir.

Anahtar Kelimeler: Anlamsal Web, ontoloji, ontoloji tabanlı bilgi sistemi, politika, erişim denetimi.

ACCESS CONTROL IN ONTOLOGY BASED INFORMATION SYSTEMS: CASE STUDY FOR NATIONAL VACCINE INFORMATION SYSTEM

Abstract

One of the main goals of the semantic web is providing information sharing and interoperability among systems and its users, by using the data of today's web which has meaning not only for human users but also for machines. Especially, ontology based information systems, which support making inferences using domain specific ontologies that have the semantics of data, have been started to develop. Information sharing provided by these systems which have huge amount of human and machine users must also provide access control and probable conflict resolution. In this work, the solutions developed in Ontology Based Access Control (OBAC) are presented to provide access control and to resolve conflicts in ontology based information systems. Role Based Access Control (RBAC) is used in existing access control applications. OBAC offers a profile based access control that is different from the applications which use role based access control, because of the additional management costs brought by RBAC. For this purpose, the personalized information is modeled semantically and it has been made the part of access control. In this work, a case study that uses OBAC, for the access control support in National Vaccine Information System which has been developed as ontology based information system with the aim of providing information and services for vaccine and vaccine applications in health domain, is given.

Keywords: Semantic Web, ontology, ontology based information system, policy, access control.

* E-posta: murat.osman.unalir@ege.edu.tr

1. Giriş

Anlamsal Web, ayrı bir web olarak düşünülmemeli, günümüzdeki webin bir uzantısı olarak algılanmalıdır. Anlamsal Web'de verinin iyi tanımlanmış anlamı ve diğer veriler ile ilişkileri verilerek bir bilgi ağı oluşturulmakta ve bu bilgi ağı kullanılarak, insanların ve bilgisayarların işbirliği içerisinde çalışmasının sağlanması ulaşılmak istenen hedef noktalardan biridir. Geliştirilen uygulamalarda veri yerine bilginin kullanılması, ontoloji tabanlı uygulamaların geliştirilmeye başlanmasına neden olmuştur. Ontoloji tabanlı uygulamalar, Anlamsal Web'de önemli bir rol oynamaktadır.

Ontoloji, kavramsallaştırılmış bir söz varlığının makinenin işleyebileceği bir biçimde sunulmasını sağlamaktadır. Ontolojiler bilginin anlamsal olarak tanımlanması için bir bütünleştirme işlemi olarak ve içeriklerin açık bir biçime getirilmesi için kullanılabilmektedirler [1]. Böylelikle, etki alanı kısıtları ve aralarındaki ilişkiler uygun bir şekilde gösterilebilmektedir.

Bilgi sistemlerinde anlamsal birlikte çalışabilirliğin sağlanabilmesi için, bilginin anlamının sistem tarafından anlaşılabilir olması gerekmektedir. Bu nedenle, bilgi sistemlerinin geliştirilmesinde, bilginin tanımlandığı ontolojiler önemli bir yere sahiptir. Birlikte çalışabilirlik, ontolojilerin anahtar bir uygulamasıdır ve birlikte çalışabilirliği gerçekleştirmek için bilgi bütünleşmesinin sağlandığı birçok ontoloji tabanlı uygulama bulunmaktadır [1]. Elektronik ticaret, maliyet yönetimi gibi alanların yanı sıra sağlık alanında da hastalara ait sağlık bilgileri üzerinden birlikte çalışabilirliğin sağlanması amacı ile farklı çalışmalar yapılmıştır.

Bilgi toplumunda bilgiye erişimin sağlanması gerekmektedir. Birçok kullanıcının bulunduğu ve her kullanıcının her bilgiye erişmemesinin gerektiği bilgi sistemlerinin başarısını arttıran en önemli kavramlardan biri de erişim denetimidir. Erişim denetimi, kullanıcıların kaynaklara erişimi ile ilgili olarak "kimin ne yapacağına" karar vermektedir. Kaynaklara yapılan yetkilendirilmemiş erişim, bilgi hırsızlığına ve bilginin bozulmasına neden olarak sistemin işleyişini etkilediği gibi, aynı zamanda mali, kanuni ve kişisel mahremiyet bakımlarından da olumsuz etkilere neden olmaktadır. Bilgi mahremiyetinin sağlanmasının önemi dikkate alındığında mobil devlet, sağlık, elektronik ticaret gibi birçok uygulamada bilgi bütünlüğünün sağlanması gerektiği görülmektedir. Bu amaçla erişim denetim politikaları kullanılmaktadır.

Günlük hayatta devlet, sağlık ve eğitim gibi birçok alanda karşılaşılan politika, sistemin davranış şeklini belirten bir durumdur. Bir sunuyu kimin, hangi koşullar altında kullanabileceğini, bilginin sunuya nasıl sağlanacağını ve sağlanan bilginin nasıl kullanılacağını belirtmektedir [2]. Sistemdeki kaynaklara ve bilgilere erişimin onaylandığını ya da reddedildiğini belirten erişim denetim kararı, politika tarafından belirlenen kurallar uygulanarak yürütülmektedir.

Bireylerin, bazı hastalıklara karşı bağışıklık kazanabilmesi veya bağışıklık düzeylerinin arttırılabilmesi için kullanılan en etkin sağlık uygulaması aşıdır. UABS (Ulusal Aşı Bilgi Sistemi), ülkemizde yaşayan her bir birey için, doğumlarından başlamak üzere, yaşamları boyunca sürecek, aşı ve aşı uygulamalarına ilişkin bilgileri kayıt altına alacak, aynı zamanda aşı ve aşı uygulamalarına ilişkin hizmetleri sunacak ontoloji tabanlı bir bilgi sistemi olarak tasarlanmaktadır. Ontoloji tabanlı bilgi sistemlerinde farklı yapıda oldukça fazla sayıdaki kullanıcının, sisteme erişim isteği UABS için de söz konusudur. UABS'nin kullanıcıları; T.C. Sağlık Bakanlığı, resmi ve özel sağlık kurumları, aşı sağlayan firmalar, eczane ve ecza depoları, aşı araştırma geliştirme laboratuarları ve okullar gibi farklı kurum ve kuruluşların yanı sıra, özel ve resmi sağlık çalışanları ile bireylerden oluşmaktadır. UABS içerisindeki kullanıcıların sisteme erişim denetimleri, sistemden alacakları hizmetlere erişimleri OBAC kullanılarak tanımlanmaktadır. UABS, Ege Üniversitesi Bilgisayar Mühendisliği bölümünde yürütülmekte olan bir çalışma olup, sistemin prototipi Ege Üniversitesi Çocuk Hastanesi'nde kullanılarak, sınanması hedeflenmektedir.

Günümüzde ontoloji mühendisliğini destekleyen çeşitli araçlar ve teknolojiler olmasına rağmen, ontoloji tabanlı uygulamaların gerçekleştirilmesi için gerekli olan mimarinin tasarlanmasında kullanılacak yönergeler bulunmamaktadır. Bu çalışmada ontoloji tabanlı bilgi sistemlerinde erişim denetiminin gerçekleştirilmesi amacı ile geliştirilen bir erişim denetimi modeli uygulaması ve bu modelin Ulusal Aşı Bilgi Sistemi uygulamasında kullanımı anlatılmaktadır. İkinci kısımda ontoloji tabanlı bilgi sistemleri ve mevcut çalışmalar hakkında bilgi verilmektedir. Üçüncü kısım klasik erişim denetim düzeneklerinden Rol Tabanlı Erişim Denetimi'ni ve bu çalışmada ontoloji tabanlı politika yönetimi için geliştirilen modelin yapısını anlatmaktadır. Ontoloji Tabanlı Erişim Denetimi modelinin kullanıldığı durum çalışması dördüncü kısımda incelenmektedir. Son olarak sonuçlar sunulmaktadır.

2. Ontoloji Tabanlı Bilgi Sistemleri

Bilgi sistemleri bilgisayarların hızla gelişmesi ile endüstride hızla kullanılmaya başlanmış ve internetin hızla yayılması sonucunda da web üzerinden kullanımın desteklenmesi sağlanmıştır. Her ne kadar bu sistemler bilgi paylaşmak ve işlemek için geliştirilmiş olsalar da, kullanılan bilgi veri seviyesinde kalmıştır. Ayrıca veri sadece sistemin insan kullanıcıları tarafından anlaşılabilmiş, sistemler arası paylaşım ise gerçekleşememiştir.

Verinin anlamını sunarak bilgiyi modellemeyi ve bilgiyi web üzerinden paylaşmayı hedefleyen Anlamsal Web'in tanımı, [3] çalışmasında "Bilginin, bilgisayarlar ve insanların birlikte çalışabilmelerini sağlayacak biçimde iyi tanımlanmış anlamının bulunduğu günümüzdeki webin genişletilmesi" olarak verilmektedir.

Anlamsal Web çalışmalarının odaklandığı temel konulardan biri de alana özgü ontolojilerin geliştirilmesi ve bunların bilgi sistemlerinde kullanılmasıdır. Kavramsallaştırmanın açık belirtimi olan ontoloji [4], kavramların tanımları ile bu kavramların birlikte etki alanı üzerinde bir yapı oluşturmak için birbirleri ile nasıl ilişkili olduklarını ve terimler arasındaki olası yorumları kısıtlayarak belirtmektedir [5]. Ontolojiler, insanlar arasındaki iletişime yardımcı olmak, bilgisayar sistemleri arasında birlikte çalışabilirliği sağlamak ve yazılım sistemlerinin süreç ve/veya kalitesini arttırmak için kullanılmaktadır [6].

Ontoloji tabanlı bilgi sistemleri, dünya ile ilgili iddialardan (assertion) oluşan bir bilgi tabanını ve bu bilgi tabanı ile muhakeme yapmak (reason) için kullanılacak bir çıkarsama motorunu içermektedirler [7]. Elektronik ticaret [8], sağlık bilgi sistemleri [9, 10, 11], maliyet yönetimi [12] gibi alanlar üzerine çeşitli uygulama çalışmaları yapılmıştır. Ontoloji tabanlı bilgi sistemlerinde, sistemin tüm bileşenlerinin ontolojiler ile tanımlanması ve sistemin sunacağı hizmetlerde kullanılacak bilgilerin ontolojik olarak tanımlanmış olması gerekmektedir. Ontoloji tabanlı bilgi sistemlerinin temel özelliklerinden biri de çok fazla sayıda kullanıcının var olmasıdır.

Ontoloji tabanlı bilgi sistemlerinde, kullanıcı sayısındaki fazlalık nedeni ile sistemler arasında bilgi paylaşımının ve birlikte çalışabilirliğin sağlanması hedeflenen asıl noktadır. Bu sistemlerde farklı kullanıcılar farklı rollere sahip olabilmektedir. Sistemde her bir role özel erişimin sağlanmasının yanı sıra, aynı rolde olan kullanıcılar arasında bile erişim şekilleri farklı olabilmektedir. Örneğin, aynı toplum sağlığı merkezinde çalışmakta olan aile hekimleri, aile hekimliği uygulamalarına erişebilirken, birbirlerinin hasta bilgilerine erişmemelidirler.

Bilgi sistemlerinin yönetimindeki en önemli gereksinimlerden bir tanesi, bilginin ve kaynakların yetkilendirilmemiş erişimlere karşı korunmasıdır. Bu nedenle sisteme, sistemin kaynaklarına ve sistemde yer alan bilgiye yapılan erişimlerin denetlenmesi ve sadece yetkilendirilmiş işlemlerin gerçekleştirilmesine izin verilmesi gerekmektedir. Bilgi sistemlerinde erişim denetiminin sağlanmasında İsteğe Bağlı Erişim Denetimi (Discretionary Access Control - DAC) [13], Zorunlu Erişim Denetimi (Mandatory Access Control - MAC) [13], Rol Tabanlı Erişim Denetim (Role Based Access Control - RBAC) [14] ve Öznitelik Tabanlı Erişim Denetimi (Attribute Based Access Control - ABAC) [15] gibi klasik erişim denetim düzenekleri kullanılmaktadır.

DAC düzeneğinde, kullanıcılar kendi kaynaklarını korumakta ve kaynak sahipleri diğer varlıklara erişim hakları verebilmektedir. DAC, uygulamadaki kolaylığı ve esnekliği nedeni ile en sık benimsenen erişim denetimi düzeneğidir. Kaynaklara erişimde, kaynağın sahibinin temel alındığı uygulamalar için DAC en uygun düzenektir. Ancak, olumsuz yetkilerin verilmesinde kısıtlı olması, izin onaylarının ve iptallerinin gerçekleştirilmesi ile ilgili işlemlerin bakımı, DAC'ın dezavantajlarını oluşturmaktadır. Ayrıca, bilginin akışında gerçek bir güvenlik sağlayamamaktadır [13]. Örneğin, bireye ait aşı kayıtlarını okuma yetkisi olan bir aile hekimi, kayıtların sahibi olan bireyin yetki vermediği başka bir bireye aşı kayıtlarını okuma yetkisi verebilmektedir. Bu problem MAC düzeneğinde önlenmektedir. MAC düzeneği, bilgi akışının sınırlandırılmasında, varlığa herhangi bir yetki vermemektedir. Kaynaklara ya da varlıklara erişim seçilmiş yöneticiler tarafından belirlenmektedir. MAC, güvenli ve merkezi bir erişim denetimi düzeneğidir. MAC'ın dezavantajı ise yöneticilik işlemlerinden kaynaklanan zorluklardır.

Rol tabanlı bir erişim denetimi düzeneği olan RBAC'da kullanıcılar rollere, izinler rollere atanmaktadır. Yönetimsel işlemler nedeni ile MAC'a benzerken, kaynak sahipliği kavramı nedeni ile de DAC'a benzemektedir. RBAC'ın yönetimi MAC ve DAC düzeneklerine göre daha kolaydır ancak kullanıcı-rol ve rol-izin atamaları maliyetlidir.
Öznitelik tabanlı erişim denetimi düzeneği olan ABAC, erişim izinleri için yeni roller tanımlamak yerine, özniteliklere göre izinleri belirlemektedir. Bu nedenle ABAC, birçok uygulamada yeniden kullanılabilecek politikaların yaratılması için kullanılabilir. ABAC erişim denetimi düzeneğinde öznelere ve özellikle kaynaklara

ilişkin özniteliklerin yapılandırılması sağlanmaktadır. RBAC düzeneğinde yer alan yönetimsel işlemler ile ilgili problemler, ABAC düzeneğinde yer almamaktadır. Ancak, kaynakların ve öznelerin anlamsal olarak temsil edilmesi ABAC tarafından sağlanamamaktadır.

Erişim denetiminin gerçekleştiriminde kullanılan politikaların, ontoloji tabanlı bilgi sistemlerinde ifade edilebilmesi için bilgi gösteriminin anlamsal bir şekilde gerçekleştirilmesi gerekmektedir. Rei [16], KAoS [17], Ponder [18], Rein [19], XACML [20], Proteus[21], WSPL[22], Protune [23] ve Appel [24] Anlamsal Web teknolojilerini kullanan politika dillerindendir. [25] çalışmasında yapılan karşılaştırmalar doğrultusunda, bu çalışmada temel alınan politika dili Rei'dir.

Rei, OWL-Lite temelli bir politika tanımlama dilidir. Kullanıcıların yetkiler, yasaklar, zorunluluklar ve özel izinler kavramlarını tanımlamasına izin vermektedir [26, 27]. Sistemdeki yetkiler ve zorunlulukların varlıklar arasında değiş tokuş edilebilmesi için, Rei politika dilinin konuşma edimleri kümesi vardır. Rei, politika tanımlamalarını çıkarsamak için bir Prolog politika motoru kullanmaktadır. Rei politika motorunun saptadığı politika çelişkilerini çözmek için ise üst veri kullanılmaktadır.

Bilgi sistemlerinde politikalar sadece sisteme olan erişimlerin denetlenmesi için değil, aynı zamanda kişiselleştirmenin sağlanması için de kullanılmaktadır. Bu amaçla, ontoloji tabanlı bilgi sistemlerinde kişiselleştirmenin sağlanabilmesi için, rol tabanlı yerine profil tabanlı bir yaklaşım tercih edilmektedir.
Bilgi sistemlerinde sunulan hizmetlerin ilgili kullanıcıya göre kişiselleştirilerek verilmesi, sistemin başarısını arttırmaktadır. Kişiselleştirme, kişiselleştirilmiş bilgi sistemlerinde bir gereksinimdir [28] ve kullanıcı beklentilerini karşılamaktadır [29]. Kişiselleştirme, ilgisiz bilginin süzülmesi ve kullanıcının benzer ilgileri ile ilgili ek bilginin tanımlanması ile sağlanabilir [28]. Kişiselleştirilmiş bir bilgi sisteminde, kullanıcılar seçimlerini tanımlamakta ve gereksinimleri doğrultusunda etki alanını sorgulamaktadırlar. Kullanıcı bağlamını ve kişiselleştirilmiş bilgi sistemini kaydetmek için kullanıcı profilleme kullanılmaktadır [30].

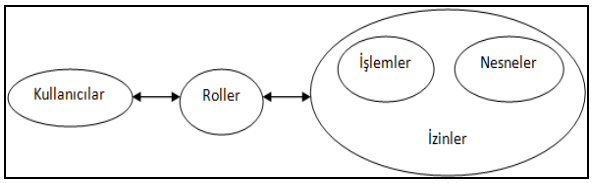
3. RBAC ve OBAC

Bilgi sistemlerinde bilginin etkin bir şekilde kullanılması, bilginin paylaşılması ile mümkün olmaktadır. Bilginin paylaşılması ile ortaya çıkan gizlilik, bütünlük ve kullanılabilirlik kavramlarının sağlanabilmesi, erişim denetim mekanizmalarının kullanılması ile mümkündür. Gizlilik, bilginin sadece yetkili kişiler tarafından okunabileceğini belirtirken, bütünlük bilginin sadece yetkili kişiler tarafından değiştirilebileceğini, kullanılabilirlik kavramı ise bilgiye ihtiyaç duyulduğunda, bilginin kullanım için uygun olduğunu ifade etmektedir.

Kullanıcı, özne, nesne, işlem ve izin kavramları herhangi bir erişim denetim düzeneğinde kullanılan kavramlardır. Kullanıcı, sistem arabirimi ile etkileşim halindedir. Kullanıcı adına hareket eden bilgisayar işlemi özne olarak adlandırılmaktadır. Nesne, sistemde yer alan dosya, yazıcı ya da veritabanı gibi erişilebilir bir kaynağı ifade etmektedir. İşlem, özne tarafından gerçekleştirilmek istenen bir süreci belirtmektedir. İzin, sistemde gerçekleştirilebilecek işlemleri belirten yetkilerdir.

Literatürde, en çok karşılaşılan erişim denetim düzeneği Rol Tabanlı Erişim Denetimi'dir (Role Based Access Control - RBAC) [31]. RBAC mekanizmasında, sistemdeki nesnelere erişim kullanıcının organizasyondaki rolüne göre gerçekleşmektedir. Rol, bir kullanıcının ya da kullanıcı grubunun bir organizasyon bağlamı içerisinde yerine getirebileceği işlemler kümesini ifade etmektedir. Sağlık etki alanında; doktor, hemşire, hasta bakıcı, eczacı gibi roller yer alabilmektedir. İşlemler, sistem yöneticisi tarafından rollere atanmaktadır. Örneğin, reçete yazmak ya da teşhis koymak doktor rolünde olan bir kullanıcının gerçekleştirebileceği işlemlerdir.

Şekil 1' de görüldüğü gibi RBAC'te, sistemde yer alan her bir kullanıcıya bir rol ve her bir rol için de işlemler ve nesneleri kapsayan izinler atanmaktadır [14]. Örneğin "Yeni Doğan Hemşiresi" rolüne sahip bir kullanıcı, "Yeni Doğan Bölümü" içerisinde yer alan "Hemşire" pozisyonunun yerine getirmesi gereken işlemler ile ilgili erişim önceliklerine ve izinlerine sahiptir.



Şekil 1. RBAC elemanları.

Sisteme bir kullanıcı dahil olduğunda, sistem yöneticisi kullanıcıya bir rol atamaktadır. Kullanıcının mevcut rolü değiştiğinde, yeni bir rol atanabilmektedir. Bir kullanıcı bir ya da daha fazla sayıda role sahip olabilmektedir. Kullanıcı, sistemden ayrıldığında ise bütün rolleri silinmektedir. RBAC'te kullanıcılar, erişim izinlerini diğer kullanıcılara aktaramamaktadır. RBAC'te erişim izinleri rollere atandığından ve sistemde yapılacak düzenleme işlemleri kullanıcılar için değil, roller için yapılacağından; yönetimsel işlemlerin aldığı yük ve zaman azalmaktadır. Ancak RBAC düzeneğinde, kullanıcı-rol ve izin-rol atamaları için yönetimsel işlemlerin gerekli olması, roller ve izinlerin sayısındaki üstel artışın kullanıcı-rol ve izin-rol atama işlemlerini daha maliyetli bir duruma getirmesi gibi bazı problemler bulunmaktadır [32].

Erişim denetim düzenekleri incelendiğinde; erişilecek kaynak, kaynağa erişen varlık (özne) ve kaynak üzerinde gerçekleştirilecek olan eylemler ön plana çıkmaktadır. Özneler, kaynaklara belirli bir amaç doğrultusunda bir eylemi gerçekleştirmek için erişmektedirler. Bu açıdan bakıldığında, Anlamsal Web için hedeflenen anlamsallık seviyesinin sağlanabilmesi için erişim denetim düzeneği içerisinde yer alan kaynak, özne ve eylemlerin anlamsal olarak temsil edilmesi gerekmektedir. RBAC düzeneğinde, özneler roller aracılığı ile temsil edilmektedir. Ancak, özneler ve kaynaklar anlamsal olarak temsil edilmemektedir. [33] çalışmasında sadece öznelerin anlamsal olarak temsil edilebilmesi amacı ile RBAC erişim denetimi düzeneği için, OWL dili kullanılarak bir ontoloji geliştirilmiştir.

Anlamsallığın sağlanabilmesi için kaynak, kaynağın sahibi ve o kaynakta gerçekleştirilmek istenen eylem bilgilerinin ontolojik olarak tutulabilmesi gerekmektedir. Bu amaçla, Ontoloji Tabanlı Erişim Denetimi (Ontology Based Access Control - OBAC) düzeneği geliştirilmiştir. Sistemin davranış biçimini belirten politikaların tanımlanmasında ontoloji dillerinden yararlanılmaktadır ve ontolojiler kullanılarak iki konu modellenmektedir: (i) erişim denetimi düzeneği (ii) kaynağın ve bu kaynağa erişmek isteyen öznenin bilgisi. OBACte; erişilecek nesne (object), bu nesne üzerinde gerçekleştirilebilecek eylemler (actions) ve bu eylemlerin hangi koşullar (conditions) altında gerçekleştirilebileceğini belirten kısıtlar, ontolojik olarak tanımlanmaktadır. Böylelikle, anlamsal olarak bütünlüğü olan parçaların yönetilmesi sağlanmaktadır.

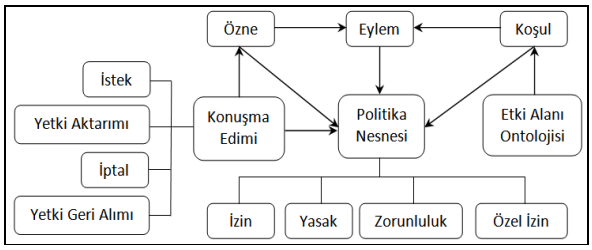
Rol tabanlı yaklaşımın getirdiği problemler nedeni ile, OBAC modelinde profil tabanlı bir yaklaşım kullanılmaktadır. Rol tanımı yapılırken, kişiye ait herhangi bir özel bilgi atanmamaktadır. Roller yaratılmakta ve kullanıcılar bu rollere atanmaktadır. Kullanıcı profili, zaman içerisinde değişebilmektedir. Örneğin, bir doktor profili nöbetçi doktor profiline dönüşebilir. Bireye ait alerjik kayıtlar kendi doktoru tarafından sorgulanabilirken, bu bireyin acil servise başvurusunda, nöbetçi doktor o bireyin doktoru olmamasına rağmen, tüm kayıtlara erişim hakkına sahip olabilmelidir. Bu iki profil arasındaki fark, rol tabanlı yaklaşımda gösterilememektedir. Ancak, kullanıcının durumunda meydana gelen bu değişikliğin, anlamsal olarak ifade edilebilmesi gerekmektedir. Ayrıca, profilde meydana gelen değişiklik modeli etkilemeyecektir. Fakat, RBAC'te kullanıcının kişisel bilgisinde meydana gelen bir değişiklik sistemi etkileyecek ve yeni rol atamalarının yapılması, yönetimsel işlemlerdeki maliyeti arttıracaktır. OBAC'te profiller kullanıcılara kişisel bilgilerine göre atanmaktadır. Eğer, kullanıcının kişisel bilgisinde herhangi bir değişiklik meydana gelirse, kullanıcının profili herhangi bir yönetimsel maliyet olmaksızın değişmekte ve bu yeni profil ile ilişkili olan politikalar işletilmektedir. Bu nedenle, OBAC'te kullanıcı verilerinde meydana gelen değişiklikler ile ilgilenmemektedir ve yönetimsel işlemler ile ilgili herhangi bir maliyet bulunmamaktadır.

Profil bilgisi oluşturulurken kişiye ait özel bilgiler dikkate alınmakta, sorgu sonuçlarının kişiselleştirilmiş olarak sunulması sağlanmaktadır. Ancak, rol bilgisini kullanarak kişiselleştirme sağlamak mümkün değildir. OBAC'te ise, kişiye ait bilgileri saklayarak ve kişiye özel bilgiyi anlamsal olarak modelleyerek, kişiselleştirme kavramı erişim denetiminin bir parçası haline getirilmektedir. Bu amaçla, sistemdeki öznelerin profilleri oluşturulmakta ve OBAC modelinin, anlamsallık seviyesinin sağlanabilmesi için de bu profiller, üst profil ontolojileri temel alınarak yaratılmaktadır.

Profil ontolojisi içerisinde kullanıcı rollerine bağlı olarak tutulan özellikler bulunmaktadır [34]. Bu özellikler FOAF (Friend Of A Friend) [35] belgelerinde tutulmaktadır. Kullanıcı profilinde yer alan kullanıcı özelliklerinin, belirli bir

aralık ve küme olarak modellenebilmesi için bir üst profil ontolojisi kullanılmaktadır. Kullanıcıları modelleyen ve kümeleyen profiller, ortak kullanıcı özellikleri, kullanıcılar arası ilişkiler gibi ayrıştırılması ve saklanması, zor bağlantıların çıkarılması ve anlamsal aramalarda kullanılabilmesini sağlamaktadır [34].

OBAC düzeneğinde tanımlanan politika bileşenleri Şekil 2'de yer almaktadır. Politika bileşenleri özne, eylem, koşul, etki alanı ontolojisi, politika nesnesi ve konuşma edimlerinden oluşmaktadır. Eylemin tanımlanmasında özne ve koşul, politika nesnesinin tanımlanmasında ise özne, eylem ve koşul kullanılmakta, koşullar oluşturulurken de etki alanı ontolojisi temel alınmaktadır. Örneğin, OBAC'in kullanıldığı durum çalışması olan UABS için etki alanı ontolojisi aşı ontolojisidir. Konuşma edimlerinin tanımlanmasında özne ve ilgili politika nesnesi kullanılmaktadır.



Şekil 2. OBAC politika bileşenleri.

OBAC düzeneğinde politika nesneleri olarak izin (permission), yasak (prohibition), zorunluluk (obligation) ve özel izin (dispensation) tanımlanmaktadır. İzin, veriye ya da sunuya erişenin neleri yapabileceğini; yasak, neleri yapamayacağını; zorunluluk, neleri yapması gerektiğini; özel izin ise neleri yapmasına gerek kalmadığını belirten durumlardır.

Farklı özneler arasındaki etkileşimlerin modellenmesi için OBAC düzeneği, konuşma edimlerini kullanmaktadır. Konuşma edimleri; istek (request), yetki aktarımı (delegate), iptal (cancel) ve yetki geri alımı (revoke) olabilmektedir. İstek, göndericinin bir eylem ya da yetki için istekte bulunması; yetki aktarımı, göndericinin alıcı için istekte bulunduğu eylem ya da yetki ile ilgili izini eklemesi; iptal, göndericinin isteği etkisiz kılması; yetki geri alımı, göndericinin vermiş olduğu izini silmesi başka bir ifade ile yasaklaması durumudur.

Politika tanımlamalarında karşılaşılan bir diğer kavram da çelişki çözümüdür. Aynı hedefteki aynı işlem için farklı kurallar/politikalar tanımlanmış olabilmektedir. Böyle bir durum ise çelişki meydana getirecektir. Birden fazla kuralın var olması durumunda, hangi kuralın uygulanacağının ya da uygulanmayacağının belirlenmesi işlemi çelişki çözümüdür. Amaç, çatışmanın sonlandırılmasıdır. Çözüm için öncelik belirlemesinden (specifying priority) ve öncelik ilişkilerinden (precedence relations) yararlanılmaktadır. RBAC modelinin desteklemediği çelişki çözümü, OBAC modeli tarafından desteklenmektedir.

Politika kuralları topluluğundan oluşan politikalar için etki alanı bilgisi temel alınmaktadır. Etki alanı politikalarında, politikalar ilgili etki alanı kurallarına göre oluşturulmaktadır. OBAC düzeneği etki alanından bağımsızdır. Kullanılan etki alanı değiştirildiğinde, sadece yaratılacak olan politikalar değişmektedir. Modelin içerisinde yapısal olarak herhangi bir durum değişikliği gerçekleşmemektedir. UABS için aşı ontolojisi etki alan ontolojisi olabilirken, turizm bilgi sistemi için etki alan ontolojisi otel ontolojisi olabilmektedir. Bu durumda, aşı ontolojisi için geliştirilen politikalar otel ontolojisi için geliştirilen politikalardan farklı ve bağımsız olacak, fakat erişim denetim modelinin genel yapısı değişmeyecektir.

OBAC düzeneğinde yaratılan politika ontolojileri Rei politika dili temel alınarak, Protégé [36] ontoloji düzenleyicisi kullanılarak oluşturulmuştur. OBAC düzeneği uygulama çatısı, Java ortamında Jena API Anlamsal Web Çatısı [37] kullanılarak gerçekleştirilmiştir. Model içerisinde yer alan sorgular ise SPARQL [38] sorgu dili ile gerçekleştirilmiştir.

4. Durum Çalışması

Sağlık alanındaki önemli uygulamalardan biri olan aşı, sonuçları ölüm veya kalıcı sakatlıklar olabilecek bazı hastalıklara karşı bireyin bağışıklık kazanabilmesi ya da bağışıklık düzeyinin arttırılması için kullanılan en etkin yöntemlerden biridir [39]. Sağlık alanının tamamında olduğu gibi, yüksek kalitede, verimli ve sürekliliği sağlanarak hizmet alma ve sunma gereksinimlerinin karşılanabilmesi, aşı ile ilgili hizmetlerin her yerde verilmesine bir başka deyiş ile coğrafik olarak dağınık olmasına ve giderek daha da özelleşen bir yapıda bulunmasına neden olmuştur. Bu

dağınık yapıda, bireylerin aşı ve aşı uygulamalarına ilişkin bilgilerinin kayıt altına alınabildiği ve sorgulanabildiği herhangi bir elektronik sistem bulunmamaktadır. Dünyada ve ülkemizde aşı ve aşı uygulamalarına ilişkin kapsamlı bir durum değerlendirmesine [40] çalışmasında yer verilmektedir. Bu çalışmada aşı ile ilgili sorunlara ontoloji tabanlı bir bilgi sistemi ile sunulabilecek çözüm ortaya konulmuş; ancak, sağlık uygulamalarında hastanın mahremiyetinin korunması ilkesine dayanarak, sağlık bilgisine erişimin nasıl denetleneceği ile ilgili bir çözüm ortaya konulmamıştır.

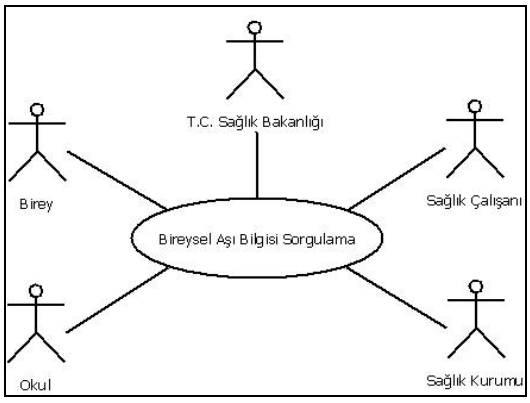
Ulusal Aşı Bilgi Sistemi (UABS) ile sağlık alanında aşı ile ilgili hem bilgi hem de kullanım hizmetlerinin yedi gün yirmi dört saat kesintisiz olarak web üzerinden verilmesi hedeflenmektedir. T.C. Sağlık Bakanlığı, resmi ve özel sağlık kurumları, eczane ve ecza depoları, aşı sağlayan firmalar, aşı araştırma-geliştirme laboratuarları, okullar gibi farklı kurumların yanı sıra sağlık çalışanları ile bireyler ve/veya anne-babaları UABS'nin paydaşlarını diğer bir ifade ile sistemin kullanıcılarını oluşturmaktadırlar. Bu kullanıcıların oluşturulmasında profil tabanlı yaklaşım kullanılmaktadır. Böylece her kullanıcı, farklı bir kullanıcı modeline sahip olmaktadır. FOAF [35] belgeleri içerisinde saklanabilen kullanıcı özellikleri kullanılarak, kullanıcı profillerinin oluşturulması esas alınmaktadır [34]. Genişletilen FOAF belgeleri içerisindeki özellikler esas alınarak oluşturulan üst profil ve profil ontolojileri kullanılarak, kullanıcı profilleri oluşturulmaktadır.

UABS durum çalışmasında yer alan paydaşlar için oluşturulan profil ontolojisinde yer alan doktor profili Şekil 3'de yer almaktadır. Burada, doktor profili için bir doktorun yaş aralığı "22-65" olarak, profilin meslek kısmı (hasOccupation) ise "Doktor" olarak belirtilmektedir.

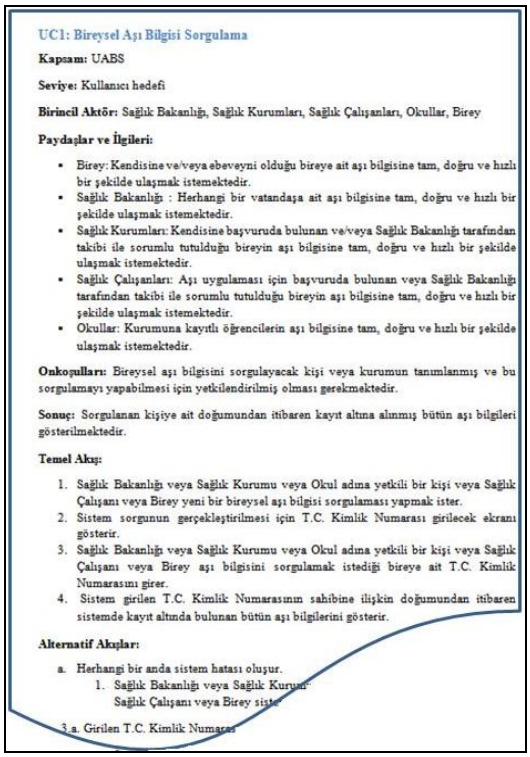
```
<metap:Age rdf:ID="DoktorYas">
  <metap:hasMinValueAge
rdf:resource="DoktorYasDegeriMin"/>
<metap:hasMaxValueAge
rdf:resource="DoktorYasDegeriMax"/></metap:Age>
<foaf:Age rdf:ID="DoktorYasDegeriMin">
  <foaf:ageValue>22</foaf:ageValue>
</foaf:Age>
<foaf:Age rdf:ID="DoktorYasDegeriMax">
  <foaf:ageValue>65</foaf:ageValue>
</foaf:Age>
<metap:Occupation rdf:ID="Doktor">
  <foaf:canbe>DoktorProfili</foaf:canbe>
</metap:Occupation>
<metap:Profile rdf:ID="DoktorProfili">
  <metap:hasName rdf:resource="DoktorAd"/>
  <hasAge rdf:resource="DoktorYas"/>
  <hasOccupation>
    <rdf:Description rdf:about="#Doktor"/>
  </hasOccupation>
 </metap:Profile>
```

Şekil 3. Doktor profili

UABS her ne kadar web üzerinden açık bir sistem olarak düşünülse de, hasta bilgilerinin mahremiyetinin korunması, bu bilgilere etik ilkeler doğrultusunda sadece izin verilen kurumlar ve kişiler tarafından erişilebilmesi gerekmektedir. Örneğin, Şekil 4'de görülen "Bireysel Aşı Bilgisi Sorgulama" kullanım durumunun kullanıcıları T.C. Sağlık Bakanlığı, sağlık çalışanı, bireyin kendisi, sağlık kurumu ve okul olabilmektedir. "Bireysel Aşı Bilgisi Sorgulama" kullanım durumunun senaryosu Şekil 5'de gösterilmektedir.



Şekil 4. Bireysel aşı bilgisi sorgulama kullanım durumu


UC1: Bireysel Aşı Bilgisi Sorgulama

Kapsam: UABS

Seviye: Kullanıcı hedefi

Birincil Aktör: Sağlık Bakanlığı, Sağlık Kurumları, Sağlık Çalışanları, Okullar, Birey

Paydaşlar ve İlgileri:

- Birey: Kendisine ve/veya ebeveyni olduğu bireye ait aşı bilgisine tam, doğru ve hızlı bir şekilde ulaşmak istemektedir.
- Sağlık Bakanlığı : Herhangi bir vatandaşa ait aşı bilgisine tam, doğru ve hızlı bir şekilde ulaşmak istemektedir.
- Sağlık Kurumları: Kendisine başvuruda bulunan ve/veya Sağlık Bakanlığı tarafından takibi ile sorumlu tutulduğu bireyin aşı bilgisine tam, doğru ve hızlı bir şekilde ulaşmak istemektedir.
- Sağlık Çalışanları: Aşı uygulaması için başvuruda bulunan veya Sağlık Bakanlığı tarafından takibi ile sorumlu tutulduğu bireyin aşı bilgisine tam, doğru ve hızlı bir şekilde ulaşmak istemektedir.
- Okullar: Kurumuna kayıtlı öğrencilerin aşı bilgisine tam, doğru ve hızlı bir şekilde ulaşmak istemektedir.

Onkoşulları: Bireysel aşı bilgisini sorgulayacak kişi veya kurumun tanımlanmış ve bu sorgulamayı yapabilmesi için yetkilendirilmiş olması gerekmektedir.

Sonuç: Sorgulanan kişiye ait doğumundan itibaren kayıt altına alınmış bütün aşı bilgileri gösterilmektedir.

Temel Akış:

1. Sağlık Bakanlığı veya Sağlık Kurumu veya Okul adına yetkili bir kişi veya Sağlık Çalışanı veya Birey yeni bir bireysel aşı bilgisi sorgulaması yapmak ister.
2. Sistem sorgunun gerçekleştirilmesi için T.C. Kimlik Numarası girilecek ekranı gösterir.
3. Sağlık Bakanlığı veya Sağlık Kurumu veya Okul adına yetkili bir kişi veya Sağlık Çalışanı veya Birey aşı bilgisini sorgulamak istediği bireye ait T.C. Kimlik Numarasını girer.
4. Sistem girilen T.C. Kimlik Numarasının sahibine ilişkin doğumundan itibaren sistemde kayıt altında bulunan bütün aşı bilgilerini gösterir.

Alternatif Akışlar:

a. Herhangi bir anda sistem hatası oluşur.
   1. Sağlık Bakanlığı veya Sağlık Kurumu
   Sağlık Çalışanı veya Birey sist

3.a. Girilen T.C. Kimlik Numarası

Şekil 5. Bireysel aşı bilgisi sorgulama kullanım durumu senaryosu

UABS için tanımlanacak politika kuralı örnekleri aşağıdaki gibidir:

- İzin: On sekiz yaşın altındaki bireylerin anne-babaları bu bireye ait aşı bilgilerini sorgulayabilirler.
- Yasak: Bir birey diğer bireylerin aşı bilgilerini sorgulayamaz.
- Zorunluluk: Sağlık çalışanı, yeni doğan bir bebeğin Hepatit B aşılaması için, annenin Hepatit B taşıyıcılık durumunu sorgulamak zorundadır.
- Özel İzin: BCG aşısı önce uygulanmış ise, kızamık içeren aşılar hemen uygulanabilir.

Durum çalışması kapsamında oluşturulan yukarıdaki izin kuralı aşağıdaki şekilde ifade edilmektedir:

Birey on sekiz yaşından küçük veya özel bakıma muhtaç bir kişi ise bu bireyin anne-babası da bireye ait aşı bilgisini sorgulama hakkına sahip olacaktır.

$$(Anne(Birey, true)) \vee Baba(Birey, true)) \wedge ((Profile(Birey) < 18) \vee (OzelBakim(Birey, true))) \rightarrow Permission(Sorgu, AsiBilgisi)$$

Ülkemizde birinci basamak sağlık hizmetlerini güçlendirmek ve verilen sağlık hizmetinin kalitesini artırmak için aile hekimi ve aile sağlığı elemanları uygulaması başlatılmıştır [41]. Bu uygulama kapsamında aile hekimi ve aile sağlığı elemanları hizmet sorumluluklarındaki bireylerin, bireysel aşı bilgisini sorgulayabilmelidir. Ayrıca, bireyler aşı hizmetini özel doktorların muayenehanelerinde veya özel poliklinikler gibi özel sağlık kurumlarından da almayı tercih edebilmektedirler. Bu durum ise, bireysel aşı bilgisi sorgulamasını yapabilecek sağlık çalışanı veya sağlık kurumunun yetkilerinin aktarılması ile sonuçlanmaktadır. OBAC'de konuşma edimleri kullanılarak, UABS'de yer alan profiller arasında yetkilerin aktarılması mümkün olmaktadır. Örneğin, Şekil 6'da özel bir sağlık kurumunda çalışan bir doktor üniversite hastanesinde çalışan bir doktordan birey ile ilgili aşı sorgularını yapabilme izini istemektedir.

```
<action:Request rdf:ID="DoktordanDoktoraIstek">
      <action:sender
          rdf:resource="Profile.owl#OzelSaglikHastanesiDoktoru"/>
      <action:content
          rdf:resource="ProfilePolicy.owl#AsiBilgisiSorgulama"/>
       <action:receiver
          rdf:resource="Profile.owl#EgeUniversitesiHastanesiDoktoru"/>
</action:Request>
```

Şekil 6. İstek konuşma edimi

Bu isteği onaylayan ve ilgili doktora aşı bilgisi sorgulama izini veren yetki aktarımı konuşma edimi ise Şekil 7'de görülmektedir.

```
<action:Delegation rdf:ID="DoktordanDoktoraYetkiAktarimi">
     <action:content
          rdf:resource="SpeechActs_DelReq.owl#İzin_AsiBilgisiSorgulama"/>
      <action:sender
          rdf:resource="Profile.owl#EgeUniversitesiHastanesiDoktoru"/>
      <action:receiver
          rdf:resource="Profile.owl#OzelSaglikHastanesiDoktoru"/>
</action:Delegation>
```

Şekil 7. Yetki aktarımı konuşma edimi

Politika kuralları tanımlanırken, bazı kuralların birbirleri ile çeliştikleri durumlar da söz konusu olabilmektedir. Örneğin, Genel Bağışıklama Programı'nda yer alan gebelik durumundaki canlı aşı uygulamasına ilişkin aşağıda belirtilen iki kural arasında bir çelişki meydana gelmektedir [42]:

- *Şeker hastası olan kişilere canlı aşılar uygulanabilir.*
- *Gebelikte canlı aşı uygulanmamalıdır.*

Eğer şeker hastası olan bir gebenin kızamık gibi bir canlı aşı olması söz konusu ise, bu iki kural birbiri ile çelişmektedir.

Çelişkinin çözülmesi için kurallar arasında öncelik ilişkileri tanımlaması yapılmaktadır. Yukarıdaki çelişki, ikinci kuralın birinci kural üzerine önceliği tanımlanarak çözülmektedir. Şekil 8, öncelik tanımlamasının yapıldığı çelişki çözümünü göstermektedir. Burada, gebelikte aşı uygulaması ile ilgili tanımlanmış yasak şeker hastaları için tanımlanmış aşı izninden daha yüksek bir önceliğe sahiptir.

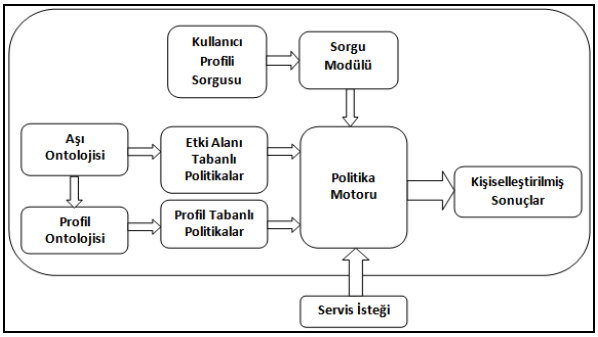
```
<metapolicy:rulePriority
rdf:ID="ProOverridesPerm_GebelikAsi">
        <metapolicy:ruleOfLesserPriority
rdf:resource="#Permission_SekerHastasiAsi"/>
        <metapolicy:ruleOfGreaterPriority
rdf:resource="#Prohibition_GebelikAsi"/>
</metapolicy:rulePriority>
```

Şekil 8. Çelişki çözümü

Ulusal Aşı Programına göre, her vatandaşın olması gereken aşıların bazılarının ilköğretim döneminde gerçekleşmesi gerekmektedir [42]. Ayrıca, eksik aşılı bireylerin belirlenerek, eksik aşılarının tamamlanması için en uygun tarama alanları da okullardır. Bu nedenle, bireyin eksik aşılarının belirlenebilmesi ve geçmiş aşı bilgilerinin sorgulanabilmesi için öğrencisi olduğu okulun da bireysel aşı bilgisini sorgulayabilmesi gerekmektedir. Bu durum OBAC'de etki alanı ve profil tabanlı politikaların sorgulanması ile gerçekleştirilmektedir.

Bu çalışmada yer alan ontolojiler, politikalar ve ontolojiler ile politikalar arasındaki ilişkiler Şekil 9'da gösterilmektedir. Burada, öncelikle, UABS'de yer alacak rolleri içeren profil ontolojisi yaratılmaktadır. Daha sonra aşı ontolojisinden ve profil ontolojisinden alınan bilgiler ile politikalar yaratılmaktadır. Politikaların yorumlanması ve çıkarsanması işlemleri politika motorunda gerçekleştirilmektedir. Sisteme gelen bir servis isteğinin cevabı ya da kullanıcı profili tarafından yapılan bir sorgu isteğinin cevabı, politika motorunun çalışması sonucunda üretilmiş kişiselleştirmiş sonuçlara göre olmaktadır.

Sistemde yer alan kaynaklar ile ilgili, 3. kısımda belirtilen 4 politika nesnesinin temel alındığı politikalar yaratılmaktadır. Bu kaynaklara erişim isteğinde bulunacak varlıklar ise profil ontolojisi ile belirtilmektedir. Kaynağa herhangi bir erişim isteği yapıldığında geliştirilmiş olan politika motoru kullanılmaktadır. Politika motoru kullanılarak gerçekleştirilen sorgu işlemine erişim isteği ile ilgili olan izin, yasak, özel izin ve zorunluluk politika nesnelerinden biri cevap olarak dönmektedir.



Şekil 9. UABS'de ontolojiler ve politikalar arasındaki ilişki

5. Sonuçlar

Bilgi teknolojilerinde ontolojilerin, bilginin paylaşılmasını ve tekrar kullanımını sağlamak amacı ile kullanılması gerekmektedir. Bilginin paylaşılması ve tekrar kullanımının sağlanması ise güvenlik kavramlarına duyulan ihtiyacı ortaya çıkarmaktadır. Oldukça büyük miktarlarda bilgi içeren bilgi sistemlerinde kişisel gizliliğin sağlanamaması durumu, hem kurumun hem de kullanıcının zarar görmesine neden olacaktır. Bu sebeple, gizliliğinin sağlanması önemli bir nokta olarak karşımıza çıkmaktadır. Ontoloji tabanlı bilgi sistemlerinde de bilgi mahremiyetinin sağlanabilmesi için, bilgiye yetkilendirilmemiş erişimin denetlenmesi gerekmektedir.

Bu çalışmada, ontoloji tabanlı bilgi sistemleri için erişim denetimini gerçekleştirmek amacıyla geliştirilen Ontoloji Tabanlı Erişim Denetim modeli anlatılmıştır. Literatürde yer alan bir çok uygulama rol tabanlı bir yaklaşıma sahip olmasına rağmen Ontoloji Tabanlı Erişim Denetim modeli profil tabanlı, bir yaklaşıma sahiptir. Bu amaçla, kişiye ait bilgiler saklanmakta ve kişiye özel bilgi anlamsal olarak modellenip, erişim denetiminin bir parçası haline getirilmektedir. Bu çalışmada, etki alanı bilgisi ve kullanıcı bilgisi anlamsal olarak temsil edilerek, ontoloji tabanlı bilgi sistemlerinin gereklilikleri yerine getirilmiş olmaktadır. Ayrıca, modelde etki alanı ontolojisi farklı ontoloji tabanlı bilgi sistemleri için farklı ontolojiler olabilmekte, bunun için sadece profillerin ve politikaların tanımlanması yeterli olmaktadır. Bu da geliştirilen modelin yeniden kullanılabilirliğini sağlamaktadır. Modelin uygulanmasında durum çalışması olarak, erişim denetiminin en sık kullanıldığı sağlık alanı için bir başka özgün çalışma olan Ulusal Aşı Bilgi Sistemi tercih edilmektedir. Durum çalışmasında izin, yasak, zorunluluk ve özel izin politika kurallarına ve profiller arasında yetki aktarımlarının gerçekleştirilmesini sağlayan konuşma edimlerine dayanarak erişim denetiminin yönetilmesi OBAC üzerinden sağlanmaktadır. Aşı uygulamalarına ilişkin kurallar arasında ortaya çıkan çelişkiler de OBAC ile çözülmektedir.

Kaynaklar

[1] Uschold,M. and Grüninger, M., "Ontologies: Principles, methods and applications", Knowledge Engineering Review, 11(2):93–155, 1996.
[2] Kagal, L., Finin, T., Paolucci, M., Srinivasen, N., Sycara, K., Denker, G., "Authorization and Privacy for Semantic Web Services", IEEE Intelligent Systems, 19(4): 50-56, 2004.
[3] Berners-Lee,T., Hendler,J., and Lassila,O., "The Semantic Web", Scientific American, vol.284, no:5, 34-43, 2001.
[4] Gruber, T., "Toward principles for the design of ontologies used for knowledge sharing", Technical Report KSL93-04, Knowledge Systems Laboratory, Stanford University, 1993.
[5] Uschold, M., "Knowledge level modelling: Concepts and terminology", Knowledge Engineering Review, 13(1), 5–29, 1998.
[6] Uschold, M., Jasper, R., "A framework for understanding and classifying ontology applications", Proceedings of the IJCA-I99 workshops on ontologies and problem-solving methods, Stockholm, Sweden, 1999.
[7] Neuhaus, F., Andersen, B., "The Bigger Picture — Speech Acts in Interaction with Ontology-based Information Systems", Interdisciplinary Ontology, Vol. 2 (Proceedings of the Second Interdisciplinary Ontology Meeting), 45-56, 2009.
[8] Zhang, L., Zhu, M., Huang, W., "A Framework for an Ontology-based E-commerce Product Information Retrieval System", Journal of Computers (JCP), Vol.4/6, 436-443, 2009.
[9] Jeong, S., Kim, H., "Design of Semantically Interoperable Adverse Event Reporting Framework", The Semantic Web - ASWC 2006, First Asian Semantic Web Conference, LNCS, vol. 4185, 588-594, 2006.
[10] Austin, M., Kelly, M, Brady, S. M., "The benefits of an ontological patient model in clinical decision-support",

AAAI'08: Proceedings of the 23rd National Conference on Artificial intelligence, 1774-1775, 2008.
[11] Suominen, O., Hyvönen, E., Viljanen, K., Hukka, E., "HealthFinland - A national semantic publishing network and portal for health information", J. Web Sem., 7(4): 287-297, 2009.
[12] Cheng, H., Lu, Y., Sheu, C., "An ontology-based business intelligence application in a financial knowledge management system", Expert Systems with Applications: An International Journal, v.36 n.2, 3614-3622, March, 2009.
[13] Sandhu, R. S., and Samarati P,"Access Control:Principles and Practice", IEEE Communications, 32 (9) 40–48, 1994.
[14] Ferraiolo, D. F., Kuhn, D. R., Chandramouli, R., Role-Based Access Control, Artech House Publishers, A.B.D., 2007.
[15] Priebe, T., Dobmeier, W., Kamprath, N., "Supporting Attributed-based Access Control with Ontologies", Proc. of the First International Conference on Availability, Reliability and Security (ARES 2006), Vienna, Austria, 465–472, 2006.
[16] Rei, http://rei.umbc.edu.
[17] KAoS, http://www.ihmc.us/research/projects/KAoS.
[18] Ponder, http://www-dse.doc.ic.ac.uk/Research/policies/ ponder.shtml.
[19] Rein, http://dig.csail.mit.edu/2006/06/rein.
[20] XACML, http://www.oasis-open.org/committees/xacml.
[21] Toninelli, A., Montanari, R., Kagal, L., Lassila, O., "Proteus: A Semantic Context-Aware Adaptive Policy Model", POLICY '07: Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks, Bologna, Italy, 13–15 June, 129 –140, 2007.
[22] Anderson, A. H., "An Introduction to the Web Services Policy Language (WSPL)", 5th IEEE International Workshop on Policies for Distributed Systems and Networks, Yorktown Heights, New York, 2004.
[23] Protune, http://rewerse.net/I2/software.html .
[24] Appel, http://www.w3.org/TR/P3P-preferences .
[25] Can, Ö., Ünalır, M. O., "Anlamsal Web Politika Dillerinin Karşılaştırması", Akademik Bilişim 2010, Muğla, 2010.
[26] 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 Conference (ISWC 2003), 419-437, 2003.
[27] Kagal, L., Finin, T., Joshi, A., "A Policy Based Approach to Security for the Semantic Web", 2nd International Semantic Web Conference (ISWC 2003), 402-418, 2003.
[28] Gauch, S., Speretta, M., Chandramouli, A., Micarelli, A., "User Profiles for Personalized Information Access", The Adaptive Web 2007, 54-89, 2007.
[29] Rich, E., "Users are individuals: Individualizing User Models", Int. J. Hum. Comput. Stud., 51(2): 323-338, 1999.
[30] Katifori, A., Golemati, M., Vassilakis, C., Lepouras, G., Halatsis, C., "Creating an Ontology for the User Profile: Method and Applications", In the proceedings of the First IEEE International Conference on Research Challenges in Information Science (RCIS), Morocco, 407-412, 2007.
[31] Can Ö., Ünalır M. O., "Ontoloji Tabanlı Erişim Denetimi", Pamukkale Üniversitesi Mühendislik Fakültesi Mühendislik Bilimleri Dergisi, Cilt 16, Sayı 2, 2010.
[32] Yuan, E., Tong, J, "Attributed Based Access Control (ABAC) for Web Services", In ICWS'05: IEEE International Conference on Web Services, 569, 2005.
[33] Finin, T. et al., "ROWLBAC - Representing Role Based Access Control in OWL", Proceedings of the 13th Symposium on Access Control Models and Technologies, 2008.
[34] Bursa, O., Ünalır, M. O., "Anlamsal Web Portallarda Profil Yönetimi", Yazılım Kalitesi ve Yazılım Geliştirme Araçları Sempozyumu 2008 (YKGS 2008), 2008.
[35] FOAF, http://www.foaf-project.org.
[36] Protégé, http://protege.stanford.edu.
[37] Jena, http://jena.sourceforge.net.
[38] Prud'hommeaux, E., Seaborne, A. , "SPARQL Query Language for RDF", http://www.w3.org/TR/rdf-sparql-query, 2008.
[39] WHO, World Health Organization, "Vaccine-preventable diseases, vaccines and vaccination", International Travel and Health, WHO Library Cataloguing-in-Publication Data, Sweeden, Chapter 6, 2008.
[40] Ünalır, E., Ünalır, M. O., Şengonca, H. ve Vardar, F., "Ulusal Aşı Bilgi Sistemi: Bir Durum Değerlendirmesi ve Yaklaşım Önerisi", Akademik Bilişim 2010, 2010.
[41] T.C. Sağlık Bakanlığı, "Aile Hekimliğinin Pilot Uygulandığı İllerde Toplum Sağlığı Merkezleri Kurulması ve

Çalıştırılmasına Dair Yönerge", 2010.
[42] T.C. Sağlık Bakanlığı, Temel Sağlık Hizmetleri Genel Müdürlüğü, "Genişletilmiş Bağışıklama Programı Genelgesi", Genelge 2009/17, 2009.