Pamukkale Üniversitesi
Mühendislik Bilimleri Dergisi
Cilt 16, Sayı 2, 2010, Sayfa 197-206

Ontoloji Tabanlı Erişim Denetimi

Ontology Based Access Control

Özgü CAN* ve Murat Osman ÜNALIR

Ege Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 35100, İzmir

Geliş Tarihi/Received : 12.11.2009, Kabul Tarihi/Accepted : 29.01.2010

ÖZET

Bilgisayar teknolojileri yaygınlaştıkça erişim denetimi düzeneklerine olan ihtiyaç da artmaktadır. Erişim denetiminin amacı, bir bilgisayar sistemi kullanıcısının gerçekleştirebileceği işlemleri sınırlandırmaktır. Böylelikle, erişim denetimi, güvenlik ihlaline neden olacak bir etkinliğin önlenmesini sağlamaktadır. Bilginin paylaşılmasını ve yeniden kullanımını sağlamak için, biçimsel anlambilimini kullanarak makinelerin diğer makineler ile iletişimine izin veren Anlamsal Web'in başarısı için erişim denetimi düzeneğine ihtiyaç duyulmaktadır. Erişim denetimi düzeneği, güvenilir bir Anlamsal Web'in sağlanması için, kullanıcının bir işlemi gerçekleştirmeden önce yerine getirmesi gereken belirli kısıtları belirtmektedir. Bu çalışmada, geleneksel erişim denetimi düzeneklerinden farklı olarak Anlamsal Web tabanlı politikaların kullanıldığı bir "Ontoloji Tabanlı Erişim Denetimi" düzeneği geliştirilmektedir. Bu düzenekte, erişim denetimi ile ilgili bilginin modellenmesi için ontolojiler kullanılmakta ve politika ontolojileri yaratılırken etki alanı bilgisi temel alınmaktadır.

Anahtar Kelimeler : *Erişim denetimi, Anlamsal web, Ontoloji, Politika.*

ABSTRACT

As computer technologies become pervasive, the need for access control mechanisms grow. The purpose of an access control is to limit the operations that a computer system user can perform. Thus, access control ensures to prevent an activity which can lead to a security breach. For the success of Semantic Web, that allows machines to share and reuse the information by using formal semantics for machines to communicate with other machines, access control mechanisms are needed. Access control mechanism indicates certain constraints which must be achieved by the user before performing an operation to provide a secure Semantic Web. In this work, unlike traditional access control mechanisms, an "Ontology Based Access Control" mechanism has been developed by using Semantic Web based policies. In this mechanism, ontologies are used to model the access control knowledge and domain knowledge is used to create policy ontologies.

Keywords : *Access Control, Semantic web, Ontology, Policy.*

1. GİRİŞ

Erişim denetimi, insanoğlu değerli varlıklarını korumaya başladığından beri var olan bir kavramdır. Bu nedenle günlük yaşamda geçitler, kilitler ve güvenlik görevlileri gibi sistemler varlıklara erişimin denetiminde kullanılmaktadır. Günümüz bilgi teknolojilerinde de en temel ve en yaygın güvenlik düzeneği olan erişim denetimi, kullanıcıların kaynaklara erişimi ile ilgili olarak "kimin ne yapacağına" karar vermektedir. Erişim denetimi farklı biçimlerde olabilir. Kullanıcının bir kaynağı kullanma iznini belirlemenin yanısıra, kaynağın ne zaman ve nasıl kullanılacağını da sınırlayabilir. Örneğin, kullanıcının kaynağa sadece belirli bir zaman dilimi içinde erişmesi tanımlanabilir. Kullanıcı, çok kullanıcılı bir sisteme her bağlandığında erişim denetimi yürütülmektedir.

Anlamsal Web, W3C (World Wide Web Consortium) tarafından örgü (web) için uluslararası standart bir gövde olarak geliştirilmiştir. Anlamsal Web girişimini ilk başlatan kişi 1989 yılında WWW'yi geliştiren Tim Berners-Lee'dir. Tim Berners-Lee, Anlamsal Web'de bilginin anlamının günümüz örgüsünde olduğundan daha önemli bir rolde olmasını beklemektedir (Antoniou ve Harmelen, 2004).

Anlamsal Web, bilginin paylaşılmasını ve yeniden kullanımını sağlamak için, biçimsel anlambilimini kullanarak, makinelerin diğer makineler ile iletişimine izin vermektedir. Böylece, bugünkü

* Yazışılan yazar/Corresponding author. E-posta adresi/E-mail address : ozgu.can@ege.edu.tr (Ö. Can)

örgüde kullanıcılar örgü sayfalarını okuyup kararlarını vermekteyken, Anlamsal Web'de ise ortak ontolojiler ve betimleme dilleri kullanılarak kullanıcıları temsil eden etmenler örgü sayfalarını okuyup anlayabilir ve karar verebilirler.

Ontolojiler varlıklar için ortak tanımlamalardır. Farklı terimleri açıklamak için ontolojilere gereksinim duyulmaktadır. Örgü sayfalarının makinelertarafından anlaşılabilir olması için ontolojiler önemlidir. Örgü bağlamında, ontolojiler bir etki alanının ortak bir anlamından söz etmektedir. Böyle bir ortak anlam, terim bilimindeki farklılıkların üstesinden gelmek için gereklidir. Örneğin bir uygulamada geçen il kodu başka bir uygulamada alan kodu olarak geçebilir. Başka bir sorun, aynı terimin her iki uygulamada farklı anlamlarla kullanılmasıdır. Örneğin, "Bilgisayar Bilimleri" bir uygulama için ders adını gösterirken, diğer bir uygulamada üniversitedeki bölümlerden birini gösterebilir. Bu tür anlamsal farklılıkların üstesinden gelmek için belirli bir terim bilimini ortak bir ontolojiye eşlemek gerekmektedir. Bu durumda görülmektedir ki, ontolojiler anlamsal birlikte işlerliği desteklemektedir.

Bilginin paylaşılması gizlilik, erişim denetimi, kimlik denetimi, yetki ve veri bütünlüğü gibi güvenlik gereksinimlerini getirmekte ve Anlamsal Web teknolojilerinin güvenliğini sağlayacak etkili düzeneklere gereksinim duyulmaktadır. Bu nedenle, Anlamsal Web ile ilgili en temel çalışmalardan biri güvenilir Anlamsal Web'in (Secure Semantic Web) geliştirilmesidir. Güvenilir Anlamsal Web ile güvenlik gereksinimlerinin sağlanması amaçlanmaktadır. Bu amaçla, kullanıcının bir işlemi gerçekleştirmeden önce yerine getirmesi gereken belli kısıtları belirten erişimi düzeneklerine ihtiyaç duyulmaktadır.

Bu çalışmada, geleneksel erişim denetimi düzeneklerinden farklı olarak anlamsal bütünlüğün sağlanabildiği Ontoloji Tabanlı Erişim Denetimi düzeneği gerçekleştirilmiştir. Bu amaçla, bu çalışmada, ikinci kısımda Anlamsal Web öncesi geleneksel erişim denetimi düzenekleri anlatılmakta ve karşılaştırılmakta, daha sonra Anlamsal Web politika dili olan Rei'den bahsedilmektedir. Üçüncü kısımda, Ontoloji Tabanlı Erişim Denetimi düzeneği anlatılmakta; dördüncü kısımda erişim denetimi düzeneklerinin karşılaştırması yapılmaktadır. Son olarak gelecekte yapılacak olan çalışmalardan bahsedilmektedir.

2. TEMEL BİLGİLER

Erişim denetimi düzeneklerinde kaynağa olan erişim kısıtlandırılmaktadır. Anlamsal Web uygulamalarında bu kısıtlandırma işlemi gerçekleştirilirken, bilginin temsilinde ontolojiler kullanılmaktadır. Ancak, geleneksel erişim denetimi düzenekleri Anlamsal Web ile uyumlu olmadıklarından, literatürde yer alan çalışmalar, Anlamsal Web öncesi ve Anlamsal Web sonrası olmak üzere iki kısımda incelenmektedir.

2. 1. Anlamsal Web Öncesi Erişim Denetimi

Aşağıda Anlamsal Web öncesi geleneksel erişim denetimi düzeneklerinden İsteğe Bağlı, Zorunlu, Rol Tabanlı, Öznitelik Tabanlı ve Kurum Tabanlı Erişim Denetimi düzenekleri sırası ile incelenmektedir.

2. 1. 1. İsteğe Bağlı Erişim Denetimi

İsteğe bağlı erişim denetimi (Discretionary Access Control-DAC) kullanıcı merkezlidir ve her bir sistem kaynağı bir ya da daha fazla varlığın sahipliğine atanmıştır. Sistem kullanıcılarının, diğer kullanıcılar tarafından kendi denetimleri altında olan nesnelere erişimine izin verip vermemesini sağlamaktadır. Erişim denetiminde kullanılan kaynak ve sahibi kavramı en genel ve gerçek dünyaya uyan bir modeldir. Bir kaynağın sahibi, kimin kaynağa erişebileceği ve hangi işlemleri gerçekleştirebileceği ile ilgili tüm kararların sahibidir. Kullanıcının nesne ile ilgili her bir isteği, belirtilmiş yetkiler kontrol edilerek gerçekleştirilmektedir (Sandhu ve Samarati, 1994). İsteğe bağlı erişim denetimi kullanıcıların sistem kaynaklarını denetleme kavramı üzerine yoğunlaşmaktadır. Gerçekleştirilmiş birçok politikanın bir şekilde ilişkilendiği isteğe bağlı erişim denetimi yaygın bir biçimde benimsenmektedir.

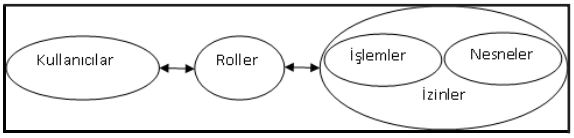
Basitlik, esneklik ve uygulamadaki kolaylığı isteğe bağlı erişim denetiminin üstünlükleridir (Benantar, 2006). DAC'ın esnekliği çok çeşitli sistemler ve uygulamalar için DAC'ı uygun kılmaktadır (Sandhu ve Samarati, 1994). Ancak, bilginin akışını ilgilendiren herhangi bir biçimsel güven sağlamaması isteğe bağlı erişim denetiminin sakıncalarındandır. İsteğe bağlı politikalarda erişim yetkilerinin dağıtılması denetimsizdir ve tüm sistemler için öngörülmesi zordur (Benantar, 2006).

2.1.2. Zorunlu Erişim Denetimi

Zorunlu erişim denetiminde (Mandatory Access Control - MAC) bir kaynağın erişim yetkileri, isteğe bağlı erişim denetiminden farklı olarak, kaynağın sahibi tarafından değil sistem tarafından belirlenmektedir. Zorunlu erişim denetimi, kaynak ve sahibi kavramını kullanmamaktadır (Benantar, 2006). Sistemdeki herbir kullanıcı ve nesne bir güvenlik seviyesi ile ilişkilendirilmektedir (Sandhu ve Samarati, 1994). Veriye erişim, yönetimsel yordamlar ile önceden tanımlanmakta ve daha sonrasında da değişmez kalmaktadır. Sistem varlıklarının veriye erişimin dağıtımına yönelik hiçbir denetimi yoktur. Bunun yerine; erişim özellikleri, güvenilir bir yönetici tarafından, her bir kaynaktaki veriye hangi kullanıcının nasıl erişeceğini belirten bir kural olarak yetkilendirilmektedir. Bir kaynağa erişmek için kullanıcının güvenlik yetkilerini tam olarak sağlaması gerekmektedir.

2.1.3. Rol Tabanlı Erişim Denetimi

Rol Tabanlı Erişim Denetimi (Role Based Access Control - RBAC) DAC ve MAC politikalarına seçenek olarak ortaya çıkmıştır. RBAC, erişim denetimini eylemde bulunan öznenin rollerine göre düzenlemektedir. RBAC düzeneğinde, güvenlik politikasının izinleri kullanıcıya değil rollere verilmektedir. RBAC ilişkileri Şekil 1'de verilmektedir (Ferraiolo v.d., 2007).

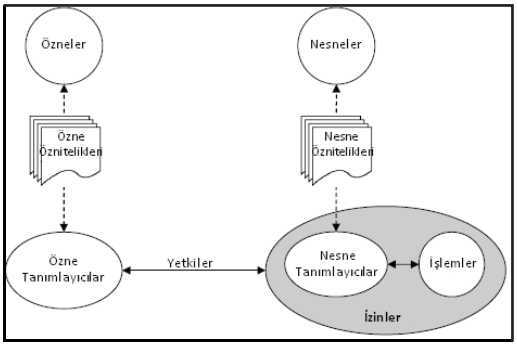


Şekil 1. RBAC ilişkileri.

Kullanıcı, izinlerini sistemde tanımlı olan rollerine göre elde etmektedir. Böylece, kullanıcı rolleri ile ilişkili olan bütün izinlerini kalıt almaktadır ve bu rol sıradüzeni ayrıca politikaların tanımlanmasını da basitleştirmektedir (Abou El Kalam v.d., 2003; Cuppens ve Miège, 2003). Örneğin, bir hastane sistemi düşünüldüğünde, hastane ağına erişebilecek roller: doktor, hemşire, laboratuvar teknikeri, memur ve yönetici; bir otel sisteminde ise varolan roller: yönetici, personel ve ziyaretçi şeklinde tanımlanmaktadır. Eğer kullanıcı personel rolünde ise kullanıcının otelin oda ile ilgili dosyalarına erişim yetkisi vardır, yönetici rolünde olan kullanıcının ise hem otelin oda dosyalarına hem de muhasebe ile ilgili dosyalara erişim yetkisi vardır. 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 (Yuan ve Tong, 2005a).

2.1.4. ÖznitelikTabanlı Erişim Denetimi

Öznitelik Tabanlı Erişim Denetimi (Attribute Based Access Control - ABAC) özneler ve nesneler arasında izinleri doğrudan tanımlamak yerine, yetkiler için onların özniteliklerini kullanmaktadır. Özneler için öznitelikler durağan olarak öznenin düzenlemedeki rolü, devingen olarak ise yaşı olabilir. Nesneler için öznitelikler ise bir belgenin konusu gibi üst veri özellikleridir. Bu kavram Şekil 2'de gösterilmektedir (Priebe v.d., 2006).



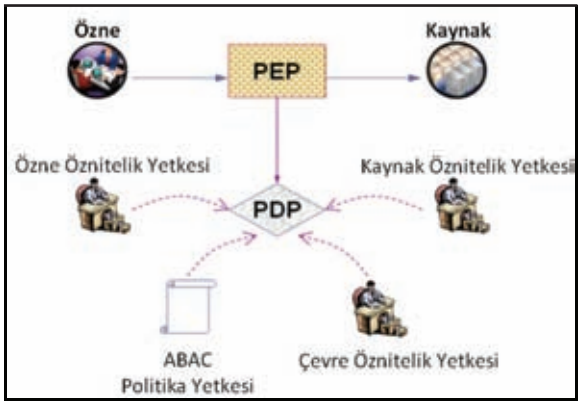
Şekil 2. ABAC düzeneğinin genel görünümü.

ABAC'da öznitelikler üç şekilde gösterilebilir. Bunlar: Özne Öznitelikleri (Subject Attributes), Kaynak Öznitelikleri (Resource Attributes) ve Çevre Öznitelikleri (Environment Attributes) (Yuan ve Tong, 2005b).

Şekil 3'de gösterilen ABAC düzeneği yapısında yer alan varlıklar Öznitelik Yetkeleri (Attribute Authorities - AA), Politika Yürütme Noktası (Policy Enforcement Point - PEP), Politika Karar Noktası (Policy Decision Point - PDP) ve Politika Yetkesi'dir (Policy Authority - PA) (Yuan ve Tong, 2005a).

Öznitelik Yetkeleri (AA), sırasıyla özneler, kaynaklar ve çevre için özniteliklerin yaratılması ve yönetilmesinden sorumludurlar. Mantıksal bir varlık olarak bir AA, öznitelikleri kendisi saklamaz, fakat öznitelikleri bir varlık ile ilişkilendirmekten sorumludur. Özniteliklerin saptanması ve elde edilmesinde önemli bir rol oynar.

Politika Yürütme Noktası (Policy Enforcement Point - PEP), yetki kararlarını istemekten ve bu kararların yürütülmesinden sorumludur. Erişim denetiminin var olabilmesinde asıl nokta PEP'tir ve bilgiyi isteyen ile bilgiyi sunan arasındaki sunu isteklerini durduracaktır. Şekil 3'de PEP tek bir nokta olarak gösterilmiş olsa da fiziksel olarak ağ boyunca dağıtık olabilir. PEP'in uygulanmasındaki en önemli nokta, korunan varlığa PEP'e uğramadan geçilemeyecek biçimde sistemin tasarlanmasıdır.



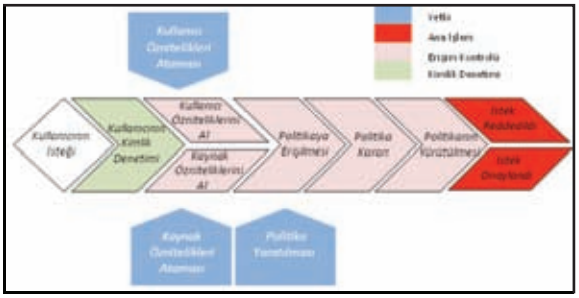
Şekil 3. ABAC yetki mimarisi.

Politika Karar Noktası (Policy Decision Point - PDP), uygulanabilir politikaların değerlendirilmesinden ve yetki kararının (onay ya da red) verilmesinden sorumludur. PDP, aslında bir politika yürütme (execution) motorudur. Bir politika istekte yer almayan bir özne, kaynak veya bir çevre özniteliğinden sözediyorsa, öznitelik değer(ler)ini elde edeceği ilgili öznitelik yetkeleri ile iletişim kurar.

Politika Yetkesi (Policy Authority - PA), erişim denetimi politikalarını yaratır ve yönetir. Politikalar, kaynaklara erişmek için, karar kurallarından, koşullarından ve diğer kısıtlardan oluşur.

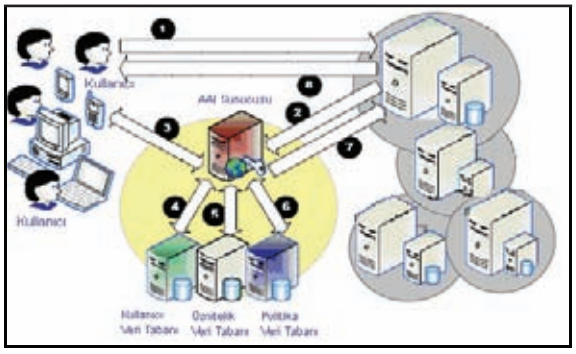
Özne Öznitelikleri, öznenin kimliğini ve niteliklerini tanımlayan özne (kullanıcı, uygulama, işlem) ile ilişkilenmektedir. Örneğin; kimlik, isim, meslek ya da rol bilgisi. Kaynak Öznitelikleri, örgü sunusu, sistem işlevi ya da veri gibi bir kaynakla ilişkilenmektedir. Örneğin; Dublin Core (The Dublin Core Metadata Initiative, 2010) üstveri elemanları. Çevre Öznitelikleri işlemsel, teknik veya durumsal çevreyi ya da bilgi erişiminin gerçekleştiği bağlamı göstermektedir. Örneğin; geçerli tarih/saat bilgisi, geçerli tehlike düzeyi.

Özne ve kaynak öznitelikleri kullanılarak kaynaklara erişimin onaylanması işlemi Şekil 4'te gösterilmektedir (Priebe v.d., 2007). Kullanıcı bir istekte bulunduktan sonra kullanıcının kimlik denetimi gerçekleştirilmektedir. Daha sonra, kullanıcı ve kaynak öznitelikleri alınıp politikaya erişilmektedir. Burada, öznitelikler kimlik ve profil bilgisi içerebilirler. Politika kararından sonra politika yürütülerek isteğin onaylanması ya da reddedilmesi işlemi gerçekleştirilmektedir.



Şekil 4. Öznitelik altyapısını kullanan güvenlik sunuları.

Öznitelik yönetimini kullanan genel bir altyapıda yer alan iletişim basamakları Şekil 5'te verilmektedir (Priebe v.d., 2007).



Şekil 5. ABAC tabanlı merkezi öznitelik yönetimi.

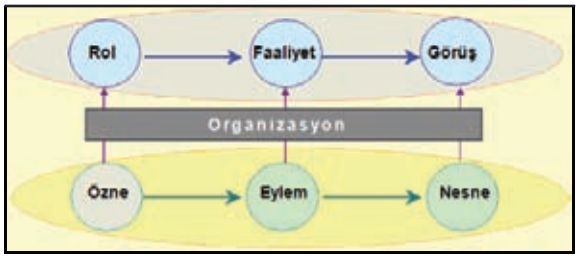
Burada gerçekleşen işlem adımları şu biçimdedir:

1. 1. Kullanıcı, sunu sağlayıcısında erişmek istediği kaynak için istekte bulunur.
2. 2. Sunu sağlayıcısı, güvenlik sunuları için Kimlik Denetimi ve Yetki Altyapı Sistemi'ni (Authentication and Authorization Infrastructure - AAI) görevlendirdiğinden, erişim denetimi kararı için istek bu sunucuya iletilir.
3. Kullanıcı kimlik denetimi gerçekleştirildikten sonra, AAI, kullanıcı özniteliklerini ortadaki bir veri tabanından alır.
4. 5. ve 6. adımlarda istek ile ilgili kararı vermek için erişim denetimi politikasını kullanır. Daha sonra, politika kararı sunu sağlayıcısına iletilir. Gerekli olması durumunda, sunu sağlayıcısı kullanıcının özniteliklerini günceller. Burada özen gösterilmesi gereken nokta kullanıcı verisinin sunu sağlayıcısında değil AAI'da saklandığıdır.

2.1.5. Kurum Tabanlı Erişim Denetimi

RBAC, DAC ve MAC gibi erişim denetimi düzenekleri politikalarının kurumlarda uygulanmasında yaşanan sorunlar nedeni ile Kurum Tabanlı Erişim Denetimi (Organization Based Access Control - OrBAC) sistemi geliştirilmiştir. Varolan erişim denetimi düzenekleri 3 varlık ile çalışmaktadır: özne (subject), eylem (action) ve nesne (object). Erişimi denetlemek amacı ile bazı öznelerin bazı nesneler üzerinde bazı eylemleri gerçekleştirmelerine izinleri olduğu politikada tanımlamaktadır. OrBAC düzeneği uygulamadan bağımsız olarak politika yazılabilmesine izin vermektedir. OrBAC sisteminde Şekil 6'da görülen iki düzey bulunmaktadır (Cuppens ve Miège, 2003):

- Somut (Concrete): özne, eylem, nesne
- Soyut (Abstract): rol (role), etkinlik (activity), görüş (view)



Şekil 6. OrBAC düzeneği düzeyleri.

Rol, kuralların uygulandığı özneler kümesidir. Etkinlik, kuralların uygulandığı eylemler kümesi, görüş ise kuralların uygulandığı nesnelerin kümesidir.

OrBAC düzeneğinde politikalar devingendir. İzin (permission), yasak (prohibition), zorunluluk (obligation) ve tavsiye (recommendation) politika nesnelerini içermektedir.

OrBAC düzeneği politikalarının kolaylıkla yaratılması amacıyla MotOrBAC (MotOrBAC, 2009) arayüzü geliştirilmiştir.

2.2. Anlamsal Web Sonrası Erişim Denetimi

Uygulamaların ve gerçek dünya senaryolarının

güvenlik ihtiyaçlarının tanımlanması ve uygulanması için erişim denetimi düzenekleri, politikalar ve diller olarak geliştirilmektedir. Aşağıda Anlamsal Web tabanlı bir politika dili olan Rei politika dili anlatılmaktadır.

2.2.1. Rei Anlamsal Web Politika Dili

Rei, OWL Lite temelli bir politika tanımlama dilidir. Kullanıcıların yetkiler, yasaklar, zorunluluklar ve özel izinler kavramlarını tanımlamasına izin vermektedir (Tonti v.d., 2003; Kagal v.d., 2003). Rei, politika geliştiricilerinin, politikaları etki alanına özgü ontolojiler üzerinde RDF (Resource Description Framework, 2004) ve OWL (Web Ontology Language) (McGuinness ve van Harmelen, 2004) gibi diller kullanarak tanımlamasına izin vermektedir. Sistemdeki yetkiler ve zorunlulukların varlıklar arasında değiş tokuş edilebilmesi için Rei politika dilinin konuşma edimleri kümesi vardır. Rei, politika tanımlamalarını çıkarsamak için de bir Prolog politika motorunu kullanmaktadır. Rei politika motorunun saptadığı politika çelişmelerini çözmek için üstveri kullanılmaktadır. Politika motoru politika tanımlarını Rei ontolojisi ile tutarlı olacak şekilde hem Rei dilinde hem de RDF-S olarak alabilmektedir (Tonti v.d., 2003). Rei politika yapısı Şekil 7'de verilmektedir.

Şekil 7. Rei politika yapısı.

Rei motoru çok çeşitli sorgulara yanıt verebilir (Kagal v.d., 2004):

- X'in Z kaynağı üzerinde Y eylemini gerçekleştirme izni var mı?
- X'in varolan zorunlulukları nelerdir?
- X, Z kaynağı üzerinde hangi eylemleri gerçekleştirebilir?
- Varolan politika etki alanında X'in bütün izinleri nelerdir?
- X'in, hangi koşullar altında Z kaynağında Y eylemini gerçekleştirme izni vardır?

2.3. Erişim Denetimi Düzeneklerinin Karşılaştırılması ve Değerlendirilmesi

Erişim denetimi düzenekleri herhangi bir bilgisayar ortamındaki bilgi akışının sınırlarını belirleyebilmek için önemlidir. Bilinen iki temel düzenek DAC ve MAC'dır. 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 erişimin sahipliği temel aldığı 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 sağlamamaktadır (Sandhu ve Samarati, 1994). Örneğin, bir dosyayı okuma yetkisi olan bir kullanıcı, okuma yetkisini, dosyanın sahibi tarafından yetki verilmemiş kullanıcılara 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 yöneticilik işlemlerinden kaynaklanan zorluklardır.

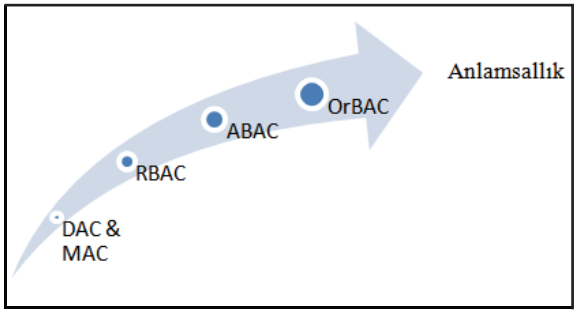
Rol tabanlı bir erişim denetimi düzeneği olan RBAC'da kullanıcılar rollere, izinler rollere atanmaktadır. RBAC, DAC ve MAC arasında bir köprü gibidir (Benantar, 2006). Yönetimsel işlemler nedeni ile MAC'a benzerken, kaynak sahipliği kavramı nedeni ile de DAC'a benzemektedir. RBAC'ın yönetimi MAC ve DAC düzeneklerine göre daha kolaydır ancak kullanıcı-rol ve rol-izin atamaları maliyetlidir.

Öznitelik tabanlı erişim denetimi düzeneği, ABAC, erişim izinleri için yeni roller tanımlamak yerine özniteliklere göre izinleri belirlemektedir. Bu nedenle, ABAC, birçok uygulamada yeniden kullanılabilecek politikaların yaratılması için kullanılabilir. Bağlam (context), bir varlığın durumunu ya da faaliyetini veya bu varlığın işlem yaptığı dünyayı niteleyen herhangi bir bilgi olarak tanımlanmaktadır (Toninelli v.d., 2007). ABAC, bağlam-farkındalığı (context-aware) yetkilerine ihtiyaç duyulduğunda, özne, kaynak ve çevre özniteliklerini kullanması bakımından uygulanacak olan en uygun düzenektir. RBAC düzeneğinde yer alan yönetimsel işlemler ile ilgili problemler ABAC düzeneğinde yer almamaktadır.

OrBAC düzeneğinde, her bir politika bir kurum için tanımlanmıştır. Bu düzenekte, diğer düzeneklerden farklı olarak izin, yasak, zorunluluk ve tavsiye politika nesneleri tanımlanabilmekte ve MotOrBAC aracı yardımı ile politika çelişmeleri çözümlenebilmektedir. Politika çelişmesi, aynı kaynak için farklı politikaların tanımlanması durumudur.

Bahsedilen bu erişim denetimi düzeneklerinin, bilginin temsil edilmesindeki anlamsallığı sağlamaları açısından gösterimleri Şekil 8'de görülmektedir. Bu şekilde, sol alt kısımdan sağ üst

kısma doğru gidildikçe, erişim denetimi düzeneği anlamsallığa yaklaşmaktadır. Anlamsallığın sağlanabilmesi için kaynak, kaynağın sahibi ve o kaynakta gerçekleştirilmek istenen eylem bilgilerinin ontolojik olarak tutulabilmesi gerekmektedir. Buna göre, anlamsallığın en zayıf olduğu erişim denetim düzenekleri, bilginin temsil gücündeki zayıflıkları nedeni ile DAC ve MAC olmaktadır. RBAC düzeneği DAC ve MAC düzeneklerinden daha çok anlamsallığa yakın olmasına rağmen kullanıcı bilgisinin rollerde tutulması nedeni ile kısıtlı bir anlamsallık sağlamaktadır. Ancak, (Finin v.d., 2008) çalışmasında RBAC düzeneği OWL Anlamsal Web tanımlama dili kullanılarak yeniden modellenmektedir. ABAC düzeneği, özne, kaynak ve çevre özniteliklerini kullanarak bilginin temsilinde anlamsallığın sağlanmasına diğer erişim denetimi düzeneklerinden daha yakındır. OrBAC ise eylem varlığınında eklenmesi ile anlamsallığa en yakın düzenek olmaktadır. Ancak, OrBAC düzeneği de RBAC'da olduğu gibi rolleri kullandığından Anlamsal Web için hedeflenen anlamsallık tam olarak sağlanamamaktadır.



Şekil 8. Erişim denetimi düzenekleri ve anlamsallık.

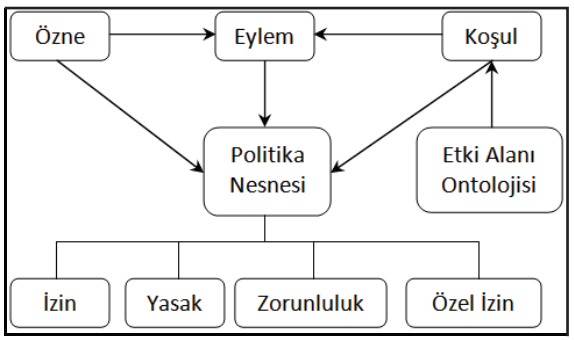
Erişim denetimi düzenekleri incelendiğinde; erişilecek kaynak, kaynağa erişen varlık (özne) ve kaynak üzerinde gerçekleştirilecek olan eylemler ön plana çıkmaktadır. Bir başka deyişle, özneler, kaynaklara belirli bir amaç doğrultusunda bir eylemi gerçekleştirmek için erişmektedirler. Bu açıdan bakıldığında Anlamsal Web için hedeflenen anlamsallık seviyesinin sağlanabilmesi için erişim denetim düzeneği içerisinde yer alan kaynak, özne ve eylemlerin anlamsal olarak temsil edilmesi gerekmektedir. Rei politika dili, eylemleri, politika nesneleri ve konuşma edimleri detayında anlamsal olarak politika üst ontolojileri aracılığı ile temsil edebilmektedir. Ancak, Rei politika dilinde, kaynak ve özneler anlamsal olarak temsil edilmemektedir. Anlamsal Web'de kaynakların ontolojik olarak yapılandırılması ile birlikte, erişim denetimi düzeneklerinde kullanımı mümkün hale gelebilecektir. Bu durumda erişim denetimi düzeneklerinin kaynakların anlamsal olarak temsil edildiği bir yapılanmayı göz önünde bulundurması gerekmektedir. RBAC ve OrBAC erişim denetimi düzeneklerinde, öznelerin, roller ve kurumlar aracılığı ile temsil edilebilmesi için gerekli yapılar sunulmaktadır. ABAC erişim denetimi düzeneğinde ise öznelere ve özellikle kaynaklara ilişkin özniteliklerin yapılandırılması sağlanmaktadır. RBAC, OrBAC ve ABAC erişim denetimi düzeneklerinin ortak amaçları kaynakların ve öznelerin temsil gücünü her bir çalışmada geliştirilen model çerçevesinde zenginleştirmektir. Ancak, bu zenginleştirmeler kaynakların ve öznelerin anlamsal olarak temsil edilmesini sağlayamamaktadır. (Finin v.d., 2008) çalışmasında sadece öznelerin anlamsal olarak temsil edilebilmesi amacı ile RBAC erişim denetimi düzeneği için OWL dili kullanılarak bir ontoloji geliştirilmiştir. Bu çalışma kapsamında geliştirilen OBAC erişim denetimi düzeneği, Rei politika dilini temel alarak, özellikle ABAC erişim denetimi düzeneğindeki yapılandırmayı anlamsallaştırmak yoluyla erişim denetimi düzeneğindeki tüm yapıtaşlarının (kaynak, özne, eylem) anlamsal olarak temsil edilebilmesini sağlamaktadır.

3. ONTOLOJİ TABANLI ERİŞİM DENETİMİ

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. Oluşturulan bu yapı Ontoloji Tabanlı Erişim Denetimi (Ontology Based Access Control - OBAC) düzeneği olarak tanımlanmaktadır. OBAC'te; 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.

RBAC ve ABAC düzeneklerinde erişilecek kaynak ile ilgili olarak herhangi bir üst veri bilgisi bulunmamaktadır. RBAC düzeneğinde erişim gerçekleştirmek isteyen öznenin bilgisi temel alınırken, ABAC düzeneğinde öznenin üzerinde işlem yapmak istediği nesneler ile ilgili öznitelikler temel alınmaktadır. OBAC düzeneğinde ise erişilecek kaynak ve bu kaynağa erişecek özne ile ilgili üst veriler anlamsal olarak oluşturulmakta, politikalar da bu üst veriler temel alınarak yaratılmaktadır.

OBAC düzeneğinde tanımlanan politika bileşenleri Şekil 9'da yer almaktadır. Politika bileşenleri özne, eylem, koşul, etki alanı ontolojisi ve politika nesnesinden oluşmaktadır. Eylemin tanımlanmasında özne ve koşul, politika nesnesinin tanımlanmasında özne, eylem ve koşul kullanılmakta, koşullar oluşturulurken ise etki alanı ontolojisi temel alınmaktadır.



Şekil 9. Politika bileşenleri.

Politikalar erişimlerin nasıl denetlendiğini ve erişim kararlarının nasıl belirlendiğini tanımlayan yüksek seviyeli yönergelerdir (Sandhu ve Samarati, 1994). Politika, politika nesnelerinden oluşan politika kurallarından oluşmaktadır. 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 durumdur.

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 bileşenleri kullanılarak yaratılan politikaların tanımlanması işlemindeki adımlar aşağıdaki gibidir:

1. Politikaya ilişkin eylemin tanımlanması.
2. Eyleme ilişkin koşulların etki alanı ontolojisi kullanılarak tanımlanması.
3. Politika nesnesinin türünün belirlenmesi.
4. Tanımlanan politika nesnesinin özne ile ilişkilendirimesinin gerçekleştirilmesi.
5. Politikanın politika deposunda saklanması.

Politika kuralları topluluğundan oluşan politikalar için etki alanı bilgisi temel alınmaktadır. Etki alanı politikalarında, politikalar ilgili etki alanı kurallarına göre oluşturulmaktadır. Durum çalışması kapsamında turizm etki alanı ontolojisi kullanılmaktadır. Turizm etki alanı ontolojisi olarak DERI tarafından geliştirilen e-turizm (E-Tourism Ontology, 2004) ontolojisi temel alınmaktadır. Oluşturulan politikaların bir kısmı şu şekildedir:

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

$$Accomodation(HiltonParis) \wedge hasRoom(HiltonParis,Guestroom) \wedge smokingAllowed\ (Guestroom,\ false) \rightarrow Prohibition(Smoking, HiltonParis)$$

Hilton Paris otelinde evcil hayvanlara izin verilmemektedir. (Yasak)

$$Accomodation(HiltonParis) \wedge petsAllowed(HiltonParis, false) \rightarrow Prohibition(OwningPet, HiltonParis)$$

Hilton Paris otelinin bütün ziyaretçileri kablosuz internet bağlantısından yararlanabilir. (İzin)

$$Accomodation(HiltonParis) \wedge wirelessConnection(HiltonParis,true) \wedge wireless\ Connection(Visitors,true) \rightarrow Prohibition(InternetAccess, HiltonParis)$$

Durum çalışması kapsamında, bu etki alanı ontolojisinin özelliklerine çeşitli eklemeler yapılarak ontoloji genişletilmiştir. Genişletilmiş turizm ontolojisi http://efe.ege.edu.tr/~ozgucan/Pamukkale/Ontoloji/I_Tour_mdfy.owl adresinde yer almaktadır. OBAC düzeneği geliştirilirken Rei üst politika ontolojileri (Rei Ontologies, 2004) kullanılmıştır. Oluşturulan politika ontolojisi http://efe.ege.edu.tr/~ozgucan/Pamukkale/Ontoloji/HotelPolicy.owl adresinde yer almaktadır.

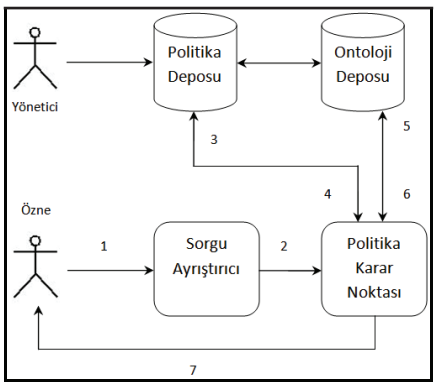
Şekil 10'da verilen OBAC mimarisinde, sistem yöneticisi tarafından oluşturulan politikalar, politika deposunda saklanmaktadır. Özne ve etki alanı bilgisini temel alan kaynak ontolojileri ontoloji deposunda yer almaktadır. Özne, bir sorgu işlemi gerçekleştirmek istediğinde, gerçekleşecek olan sorgu adımları aşağıdaki gibidir:

1. Özne, etki alanı ontolojilerini kullanarak sorgusunu yazar.
2. Sorgu, Sorgu Ayrıştırıcı tarafından koşullarına ayrılır ve bu koşullar Politika Karar Noktasına iletilir.

3-4. Herbir koşul için Politika Karar Noktası tarafından, politika deposu kullanılarak, ilgili politikalar belirlenir.

5-6. Politika nesnesinin türüne göre Ontoloji Deposundan ilgili veri çekilir.

7. Özneye sorgu sonucu döndürülür.



Şekil 10. OBAC mimarisi.

Özne, sorgu işlemini gerçekleştirirken sistemde yer alan politikalardan habersizdir. Özne sadece kendi sorgusunu yazmaktadır. Örneğin, özne, internet erişimi izini olan otelleri sorguladığında "hasInternetAccess=true" koşulu kullanılarak, etki alanı ontolojisinde bu koşulu sağlayan otellerin listesi özneye döndürülecektir.

Burada dikkat edilecek bir diğer nokta, OBAC düzeneğinin etki alanından bağımsız olmasıdır. Kullanılan etki alanı değiştirildiğinde sadece yaratılacak olan politikalar değişmektedir. Modelin içerisinde yapısal olarak herhangi bir durum değişikliği gerçekleşmemektedir. Ayrıca, gelişen Anlamsal Web teknolojileri dikkate alındığında, erişilecek kaynağı temsil eden etki alanı ile ilgili bir çok kaynağa, Swoogle (Swoogle, 2010); Watson (Watson, 2010) gibi Anlamsal Web arama motorları kullanılarak kolaylıkla ulaşılabilmektedir.

Rei politika dili, sadece üst politika ontolojilerinden oluşmaktadır. Bu ontolojilerin nasıl kullanılacağı ile ilgili herhangi bir bilgi ya da ontolojilerin kullanıldığı herhangi bir uygulama çatısı sunmamaktadır. Rei'nin aksine, OBAC düzeneği uygulama çatısı, Java ortamında Jena API (Jena, 2010) Anlamsal Web Çatısı kullanılarak gerçekleştirilmiştir. Model içerisinde yer alan sorgular SPARQL (Prud'hommeaux ve Seaborne, 2008) sorgu dili ile gerçekleştirilmiştir.

4. RBAC, ABAC VE OBAC KARŞILAŞTIRMASI

Anlamsal Web teknolojilerine dayanan politika dilleri, politikaların heterojen etki alanı verileri üzerinde tanımlanmasına izin vermekte ve aynı bilgi modelini kullanmayan katılımcılar arasında ortak anlamı desteklemektedir (Finin v.d., 2008). Son yıllarda yapılan erişim denetimi çalışmalarında iki paralel konu ele alınmaktadır (Finin v.d., 2008): gerçek dünya uygulama etki alanlarının politika gereksinimlerini karşılamaya yönelik erişim denetimi düzeneklerinin geliştirilmesi ve erişim denetimi için politika dillerinin geliştirilmesi. Bu iki paralel konunun, erişim denetimi ve politika dilleri, güvenlik altyapısının gelişimini sağlamak için görevdeşlik yaratması gerektiği düşünülmektedir. OBAC düzeneğinde politika yönetimi ile erişim denetimi birleştirilmektedir. Mevcut erişim denetimlerinde olmayan bu nokta, bu çalışmanın en önemli katkılarından biridir.

OBAC düzeneğinde önerilen çözüm, erişim denetimi kavramlarının politika dilleri tarafından desteklenen modeller içerisinde doğal bir şekilde belirtilmesi ve modellerin ötesindeki detayların ise politika dili içerisinde ayrıca belirtilmesine izin verilmesidir.

RBAC düzeneğinde, güvenlik politikası izinleri, kullanıcıya değil rollere verilmektedir. Kullanıcı, izinlerini sistemde tanımlı olan rollerine göre elde etmektedir. Böylece, kullanıcı rolleri ile ilişkili olan bütün izinlerini kalıt almaktadır ve bu rol sıradüzeni ayrıca politikaların tanımlanmasını da basitleştirmektedir (Cuppens ve Miège, 2003).

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 masraflı bir hale getirmesi gibi bazı olumsuzluklara neden olmaktadır (Yuan ve Tong, 2005a). RBAC düzeneğinin yönetiminde, rollere kullanıcı ve izin atamalarının nasıl yapıldığı konusunda bir ayrıntı bulunmamaktadır (Finin v.d., 2008).

ABAC, özneler ve nesneler arasında izinleri doğrudan tanımlamak yerine, yetki tanımlamaları için onların özniteliklerini kullanmaktadır. ABAC yaklaşımında, rollerin tanımlanmasına gerek yoktur. Bu durum RBAC'dan farklılık göstermektedir. Bu açıdan bakıldığında, ABAC düzeneğinin üstünlüğü rollerin tanımlanması ve yönetimi işlemlerini yok etmiş olmasıdır. Böylece, kullanıcı-rol ve izin-rol atamaları için gerekli olan yönetim görevleri de ortadan kalkmaktadır (Jrad ve Aufare, 2007).

OBAC'da; erişilecek nesne, bu nesne üzerinde gerçekleştirilebilecek eylemler ve bu eylemlerin hangi koşullar altında gerçekleştirilebileceğini belirten kısıtlar ontolojik olarak tanımlanmaktadır. OBAC'ın sunduğu bu model Finin tarafından gerçekleştirilen çalışmada (Finin v.d., 2008) ifade edilen gereksinimi karşılamaktadır. Böylelikle, anlamsal olarak bütünlüğü sağlanması gereken ontoloji tabanlı erişim denetimi ve politika yönetimi sağlanmaktadır. RBAC ve ABAC düzeneklerinde erişilecek kaynak ile ilgili olarak herhangi bir üst veri bilgisi bulunmamaktadır. RBAC düzeneğinde erişim gerçekleştirmek isteyen öznenin bilgisi temel alınırken, ABAC düzeneğinde öznenin üzerinde işlem yapmak istediği nesneler ile ilgili öznitelikler temel alınmaktadır. OBAC düzeneğinde ise erişilecek kaynak ve bu kaynağa erişecek özne ile ilgili üst veriler anlamsal olarak oluşturulmakta, politikalar da bu üst veriler temel alınarak yaratılmaktadır.

RBAC ve ABAC düzeneklerinde bir sistemdeki bütün politika ayrıntılarının ifade edilmesini sağlayacak düzenek bulunmamaktadır. RBAC düzeneğinde roller, isimlendirilmiş varlıklar olarak tanımlanabilmektedir. Bu durumun ontolojik olarak bir anlamsallığı bulunmamaktadır. Örneğin "genç akademisyen" tanımı yapılmak istendiğinde RBAC düzeneğinde, "genç" ve "akademisyen" tanımlamaları ayrı ayrı yapılabilirken bu iki tanımı birleştiren "genç akademisyen" durumu belirsiz kalmaktadır. OBAC düzeneğinde ise "genç" ve "akademisyen"tanımlarıyapılırken,butanımlarsadece isimlendirilmiş birer varlık olarak alınmamaktadır. "Genç" tanımı için yaş bilgisi, örneğin; 18 ile 35 yaş arası olmak üzere sınırlandırılmaktadır. Aynı şekilde, "akademisyen" tanımı yapılırken ise meslek bilgisi temel alınmaktadır. "Genç akademisyen" tanımı, ontoloji modelindeki kesişim mantıksal operatörü ile sağlanmaktadır. RBAC düzeneğinde, rol tanımı ontolojik olmadığından roller arasındaki ilişkiler tanımlanamamaktadır. OBAC düzeneğinde ise bu durumun tanımını ontolojik olarak yapmak mümkündür.

RBAC ve ABAC düzeneklerinde politika nesneleri sadece izin ve yasak şeklinde tanımlanırken OBAC düzeneğinde izin, yasak, zorunluluk ve özel izin şeklinde olması OBAC modelinin RBAC ve ABAC düzeneklerine olan bir diğer üstünlüğünü oluşturmaktadır. Buna ek olarak, RBAC ve ABAC modellerinde konuşma edimleri ile ilgili bir destek bulunmamaktadır. OBAC düzeneği ise istek, yetki aktarımı, iptal ve yetki geri alımı olmak üzere 4 konuşma edimini de desteklemektedir.

RBAC düzeneğini temel alan Chen tarafından gerçekleştirilen çalışmada (Chen, 2008), bilgiye erişimi ontoloji tabanlı erişim denetimi ile gerçekleştirilmektedir. Bu çalışma, bilgi içeriğini tanımlamak için bilgi kavramlarını ve ilişkilerini ontoloji tabanlı bir yaklaşım ile modellemektedir. Oluşturulan ontolojiler ürün etki alanını, rolleri ve süreçler arası ilişkileri tanımlamaktadır. Ancak, bu çalışmada sadece erişim denetimi izinlerinin tanımlanması sağlanmaktadır.

Sun v.d., (2007) ise RBAC düzeneğini temel alan bir diğer ontoloji tabanlı erişim denetimi çalışmasıdır. Bu çalışmada, yetki kuralları için ortak bir ontoloji tanımlanmaktadır. Sisteme kayıtlı kullanıcılar politikalar ve yetkiler kullanarak kendi kaynaklarının izinlerini belirlemektedirler. Sisteme kayıtlı kullanıcılar arasında uyumun sağlanması ve dışardan gelen sorgulara cevap verebilmek için kullanıcıların kendi yerel yetkileri ile ortak ontoloji arasında eşlemeler yapılmaktadır. Bu çalışmada, erişim denetiminde sadece izinleri kullanmaktadır.

RBAC, ABAC ve OBAC düzeneklerinin karşılaştırması Tablo 1'de yer almaktadır. Bu çizelgede, karşılaştırma, politika tanımlamada önemli bir yeri olan rol tanımı, politika nesneleri ve konuşma edimleri açılarından yapılmaktadır.

Tablo 1. RBAC, ABAC ve OBAC karşılaştırması.

	RBAC	ABAC	OBAC
Rol Tanımı	Rol tabanlı	Öznitelik tabanlı	Ontoloji tabanlı
Politika nesneleri	İzin ve yasak	İzin ve yasak	İzin, Yasak, Zorunluluk ve Özel izin
Konuşma edimleri	Yok	Yok	İstek, Yetki aktarma, İptal ve Yetki geri alma

Bu tabloda; rol tanımı, modelin temel aldığı yapıyı belirtmektedir. RBAC düzeneği rol tabanlı, ABAC ise öznitelik tabanlı bir modeldir. OBAC düzeneği ise ontoloji tabanlı bir modeldir. RBAC ve ABAC, politika nesneleri olarak sadece izin ve yasak tanımlarken OBAC düzeneğinde bu nesnelere ek olarak zorunluluk ve özel izin tanımlanmaktadır. Konuşma edimleri sadece OBAC düzeneği tarafından desteklenmektedir.

5. SONUÇLAR VE GELECEK ÇALIŞMA

Bu çalışmada, Anlamsal Web teknolojilerinde erişim denetimi düzeneğinin gerçekleştirilebilmesi için Anlamsal Web politika dili kullanılarak ontoloji tabanlı bir erişim denetimi düzeneği geliştirilmiştir. Bu amaçla; Anlamsal Web öncesi erişim denetimi düzeneklerinden, Anlamsal Web politika dili kullanılarak geliştirilen Ontoloji Tabanlı Erişim Denetimi düzeneğinden ve bu düzenekte yer alan politikaların turizm etki alanı ontolojisini temel aldığından bahsedilmiştir. Mevcut erişim denetimi düzeneklerinden RBAC ve ABAC ile geliştirilen Ontoloji Tabanlı Erişim Denetimi düzeneği karşılaştırılmıştır.

Ontoloji Tabanlı Erişim Denetimi düzeneğinin kullanıcı arayüzü ve politika çıkarsama motoru Jena API kullanılarak Eclipse (Eclipse, 2010) ortamında geliştirilmiş, SPARQL kullanılarak çeşitli sorgular gerçekleştirilmiştir.

OBAC düzeneği bir çok etki alanına uygulanabilmektedir. Etki alanı değiştikçe politikalar yeni etki alanına göre yaratılacaktır. Etki alanının değişmesi halinde düzeneğin çalışmasını etkileyen herhangi bir durum ortaya çıkmamaktadır. Bu çalışmada geliştirilen durum çalışması, turizm etki alanını kapsamaktadır. Bundan sonra yapılacak çalışmalar için uygulama alanı değiştirilecek ve başka etki alanları da durum çalışmasına eklenerek uygulama alanı genişletilecektir.

KAYNAKLAR

Abou El Kalam, A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte,Y., Miège, A., Saurel, C. and Trouessin, G. 2003. "Organization Based Access Control" **IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003),** Lake Come, Italy, June 4-6.

Antoniou, G. and van Harmelen, F. 2004. A Semantic Web Primer 238s. The MIT Press, Cambridge, MA, USA, ISBN 0-262-01210-3.

Benantar, M. 2006. Access Control Systems Security, Identity Management and Trust Models. Springer Science Business Media 261s. Springer-Verlag New York, Inc., Secaucus, NJ, ISBN: 978-0-387-00445-7.

Chen, T.Y. 2008. Knowledge sharing in virtual enterprises via an ontology-based access control approach. Computers in Industry. 59 (5), 502–519.

Cuppens, F. and Miège, A. 2003. "Modelling Contexts in the Or-BAC Model" **19th Annual Computer Security Applications Conference.**

Eclipse. 2010. http://www.eclipse.org.

E-Tourism Ontology. 2004. http://e-tourism.deri.at/ ont/e-tourism.owl .

Ferraiolo, D. F., Kuhn, D. R., Chandramouli, R. 2007. Role Based Access Control. Artech House Publishers, Second Edition, ISBN 13: 978-1-59693-113-8.

Finin, T. et al. 2008. "ROWLBAC - Representing Role Based Access Control in OWL" **Proceedings of the 13th Symposium on Access Control Models and Technologies.**

Jena. 2010. http://jena.sourceforge.net.

Jrad, Z. and Aufaure, M.A. 2007. "Personalized Interfaces for a Semantic Web Portal. Tourism Information Search" **In KES 2007/WIRN 2007,** Part III, LNAI 4694. pp. 695-702.

Kagal, L., Finin, T. and Joshi, A. 2003. "A Policy Based Approach to Security for the Semantic Web" **2nd International Semantic Web Conference (ISWC 2003). pp. 402-418.**

Kagal, L., Finin, T., Paolucci, M., Srinivasen, N., Sycara, K. and Denker, G. 2004. Authorization and Privacy for Semantic Web Services. IEEE Intelligent Systems. July/Aug. 2004, doi:10.1109/MIS.2004.23. 19 (4), 50-56.

McGuinness, D. L. and van Harmelen, F. 2004. "OWL Web Ontology Language Overview" http://www.w3. org/ TR/owl-features .

MotOrBAC. 2009. http://motorbac.sourceforge.net .

Priebe, T., Dobmeier, W. and Kamprath, N. 2006. "Supporting Attributed-based Access Control with Ontologies" **Proc. of the First International Conference on Availability, Reliability and Security (ARES 2006),** Vienna, Austria. pp. 465–472.

Priebe, T., Dobmeier, W., Schläger, C. and Kamprath, N. 2007. Supporting Attribute-based Access Control in Authorization and Authentication Infrastructures with Ontologies. Journal Of Software (JSW). ISSN: 1796-217X. 2 (1), 27-38.

Prud'hommeaux, E. and Seaborne, A. 2008. "SPARQL Query Language for RDF" http://www.w3.org/TR/ rdf-sparql-query .

Rei Ontologies. 2004. http://www.cs.umbc.edu/ ~lkagal1/rei/ ontologies.

Resource Description Framework. 2004. http://www. w3.org, / RDF .

Sandhu, R. S. and Samarati P. 1994. Access Control:Principles and Practice. IEEE Communications. 32 (9) 40-48.

Sun, Y., Pan, P., Leung, H. and Shi, B. 2007. "Ontology Based Hybrid Access Control for Automatic Interoperation" **4th International Conference, ATC 2007,** Hong Kong, China, July (11-13), 323-332.

Swoogle. 2010. http://swoogle.umbc.edu.

The Dublin Core Metadata Initiative. 2010. http://dublincore.org .

Toninelli, A., Montanari, R., Kagal, L. and Lassila, O. 2007. "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 2007. pp.129 –140.

Tonti, G., Bradshaw, J. M., Jeffers, R., Monranari, R., Suri, N. and Uszok, A. 2003. "Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KaoS, Rei, and Ponder" **2nd International Semantic Web Conference (ISWC 2003).** pp. 419-437.

Yuan, E. and Tong, J. 2005a. "Attributed Based Access Control (ABAC) for Web Services" **In ICWS'05: IEEE International Conference on Web Services,** pp. 569.

Yuan, E. and Tong, J. 2005b. "Attribute Based Access Control - A New Access Control Approach for Service Oriented Architecture (SOA)" **New Challenges for Access Control Workshop,** Ottawa, ON, Canada, April 27.

Watson. 2010. http://watson.kmi.open.ac.uk/ WatsonWUI .