Melez Erişim Denetimi için bir Mimari Önerisi: İK Uygulaması Örneği

Nuriye Yasemin Alparslan[1], Murat Komesli[1], Murat Osman Ünalır[2], Özgü Can[2]

[1] Yaşar Universitesi Yazılım Mühendisliği Bölümü
Üniversite Cad. 35, 35100, Bornova, İzmir, Türkiye
{nuriye.alparslan, murat.komesli}@yasar.edu.tr

[2] Ege Universitesi Bilgisayar Mühendisliği Bölümü
Üniversite Cad. 9, 35100, Bornova, İzmir, Türkiye
{osman.unalir, ozgu.can}@ege.edu.tr

Özet. Anlamsal web, web içeriklerinin diğer yazılımlar tarafından anlaşılabilir, yorumlanabilir, kullanılabilir olmasını ve bilginin paylaşılmasını amaçlamaktadır. Anlamsal web'de bilginin güvenliği erişim denetimi ile sağlanmaktadır. OBAC(Ontology Based Access Control – Ontoloji Tabanlı Erişim Denetimi) verinin anlamsal tanımının olduğu ontolojilere erişim denetiminin sağlanmasında kullanılan bir modeldir. RBAC(Role Based Access Control – Rol Tabanlı Erişim Denetimi) ise, rol tabanlı erişim denetimini sağlamaktadır. İlişkisel veritabanlarında RBAC, ontolojilerde ise OBAC kullanılmaktadır. İnsan Kaynakları (İK) uygulamalarında hem RBAC hem de OBAC kullanılmaktadır. Bu çalışmada, her iki yaklaşımın karışımı olan HAC (Hybrid Access Control- Melez Erişim Denetimi) altyapı mimarisi geliştirilmeye çalışılmıştır. İK alanında, OBAC ve RBAC birleşimiyle oluşan melez veri tabanlı bir erişim çerçevesi olarak HAC geliştirilmektedir. Bu çerçeveye erişim için, yöntem ve araç yazılım içeren bir yazılım mimarisi sunulmaktadır. Böylelikle, melez veri ile roller yönetilerek İK alanında veritabanı yönetimine bir çözüm getirilmiş olacaktır.

Anahtar Kelimeler: RBAC, OBAC, HAC, Erişim Çerçevesi.

1 Giriş

Organizasyonların performansının artması için insan kaynakları yönetimi ile iş gücü ve kaynak planlamasının verimli kullanılması gerekmektedir. İK alanında çalışanlar, iletişim kanalı olarak web teknolojisini fark ettikten sonra, işe-alım süreçlerinde anlamsal olarak dağınık bulunan bilgiye erişim ve paylaşım büyük ölçüde sağlanmıştır. Sonrasında, İK için ortak bir sözlük belirlenmiş ve insan kaynakları ontolojisi oluşturulmuştur [1]. İşealım süreçlerinde aday ve çalışanların bilgilerinin kurumlararası kullanımı ve paylaşımı, insan kaynakları alanında bazı tanımların standartlaştırılması ihtiyacını doğurmuştur. Bu ihtiyaç doğrultusunda, insan kaynakları ile ilişkili bilginin kurumlar arası paylaşımı ve ortak tanımları için birbirinden farklı XML-Şema tanımları yapılmıştır [2]. İK Açık Standartları (HR

Open Standards), İK profesyonelleri ve teknoloji uzmanları tarafından geliştirilmiştir. Böylece yeni standartlar oluşturularak İK alanında veri bütünleştirmesi sağlanmaktadır[3].

Oluşturulan standartlar doğrultusunda, paylaşılan ve makinalar tarafından anlaşılan bilgiye erişimin güvenliği sağlanmış olmalıdır. Bilgi teknolojilerinde güvenlik, Erişim Denetimi ile sağlanmaktadır. Erişim çerçevesi hangi kullanıcının hangi kaynağa hangi erişim yetkisinde ulaşabileceğinin sınırlarını çizmektedir. Erişim çerçevesi kapsamında, kullanıcılara verilen hakların gözden geçirilmesi, kullanıcıların belli dosyalara erişiminde yazma, okuma gibi izinlerinin yönetilmesi ile bilginin ve kaynakların güvenliği sağlanmaktadır. Anlamsal web ile makinelerin diğer makinelerle iletişimi sağlanarak, bilginin paylaşılması ve yeniden kullanılabilir olması amaçlanmaktadır[4]. Anlamsal web teknolojileri, bilginin paylaşılması ve yeniden kullanılabilir olması ve devamında veri bütünlüğünün sağlanabilmesi için gizlilik ve güvenlik konularını gündeme getirmektedir [5].

Erişim denetiminde kaynağa olan erişimin kısıtlanması, farklı düzeneklerle sağlanabilmektedir. RBAC ile kaynağa erişimde izin ve yetkiler kullanıcının kendisine değil, rollere verilmektedir. Dolayısıyla, bir kullanıcı rollerle ilişkilendirildiğinde, rollere verilen yetki ve izinlere sahip olur [6]. OBAC ile kaynağa erişimde üst veri kullanılmaktadır. Politikalar üst veri ve kaynağa erişecek özne arasında anlamsal olarak oluşturulmaktadır [5].

Bu çalışmada, veriye ulaşmada anlamsal bütünlüğün sağlanabildiği ontoloji tabanlı erişim denetimi (OBAC) ile, ilişkisel model olarak rol tabanlı erişim denetimi (RBAC) birleşimi sonucu oluşan Melez Veri Tabanlı erişim kontrolü için bir mimari önerisi sunulmaktadır. Böylece, rollerin yönetimi ve veritabanı yönetimine getirilen çözüm mimarisi anlatılmış olacaktır. İkinci bölümde bu konuda yapılan çalışmalarda ve araştırmalarla ilgili geniş bilgi verilmektedir. Üçüncü bölümde melez veri tabanlı erişim için İK senaryosu dahilinde bir yapı önerilmektedir. Son bölümde ise konu ile ilgili sonuç ve önerilere yer verilmiştir.

2 Literatür Araştırması

Ontolojiler bilgi gösteriminin daha güçlü formu olarak kavramlar arasındaki ilişkileri ve kısıtları açıklamaktadır. İnsan kaynakları alanı için oluşturulan ontolojiler, yetkinlik, iş tanımı gibi mutlak kavramlar ve bu kavramların birbiriyle olan ilişkilerini içermektedir. Tipik işealım süreçleri ve aday önerileri anlamsal web aracılığıyla yapılabilir hale gelmiştir. HR-XML Konsorsiyum aracılığıyla geliştirilmiş olan HR-XML işaretleme dili, insan kaynakları ontolojisi için 75'ten fazla birbirinden bağımsız XML şema içermektedir [7]. İnsan kaynakları alanında yapılan bazı anlamsal web içerikli çalışmalar sonraki bölümlerde açıklanmaktadır.

2.1 Ecco Sistem Uygulaması

Ecco projesi İtalyan endüstri ortakları (AICA ve Federcomin) ve Milan Teknik Üniversitesi tarafından İtalya hükümeti desteği ile geliştirilmiş bir projedir. Yetenek ve iş profilleri konusunda şeffaflık, karşılaştırılabilirlik, bilgi ve yönlendirme sağlanması amaçlanmıştır. Ecco projesi ulusal ve uluslararası ICT(Information and Communication Technologies) yetenek ve iş profilleri yaklaşımlarının analizleriyle başlamıştır. Ecco projesinde yetenek tanımı için bilgi (knowledge), bilgi nesnesi (knowledge object), birşeyi yapabilmek anlamına gelecek şekilde yetenek (skill), belli bir alana ait yetenek (competence), performans ve iş profili gibi ana tanımlamalar bulunmaktadır.[8]. Tanımladığı standartlarla yetenek tanımlarını açıklamak, referans vermek, tekrar kullanılabilir olmasını sağlamak için bir veri modeli oluşturmuştur [9].

2.2 Kowien

Kowien (Kooperatives Wissensmanagement in Engineering-Netzwerken/ Cooperative Knowledge Management in Engineering Networks) bilgi tabanlı sistem alanında ortak bir araştırma projesidir. Kowien ontoloji tabanlı bilgi sistemini, çalışanların yeteneklerine göre organizasyondaki yerini belirlemek için kavramsallaştırmakta, geliştirmekte ve değerlendirmektedir. Bu amaca ulaşmak için kurumun tüm ilgili bilgi kaynakları çalışanların yetenekleri ile ilgili bilgi tabanı oluşturmak için kullanılmaktadır[10]. Kowien, iş pozisyonu gereksinimlerini ve iş başvurularında gelen yetenekleri tanımlamak için gereken yetenek kavramlarının tanımlandığı bir yetenek ontolojisidir[11].

2.3 Erişim Denetim Mekanizmaları

Anlamsal web öncesi ve sonrası geliştirilmiş olan erişim denetimi düzenekleri şunlardır:

2.3.1 DAC (Discretionary Access Control - İsteğe Bağlı Erişim Denetimi)

DAC politikasında kullanıcılar diğer kullanıcılara izin ve yetki verir, yani erişim denetimi kullanıcı merkezlidir. Bu şekilde dağınık veri üzerinde erişim kontrolü yönetilebilir. DAC politikasında bir veya birden fazla kaynağa erişim hakkı olan kullanıcı, bir veya birden fazla özneye bu kaynağa erişim ve işlem yapmak için yetki verebilir. [12]. DAC Erişim modelinin diğer erişim modellerine göre üstünlükleri esneklik, uygulamadaki kolaylığıdır. Erişim yetkilerinin dağıtılmasının denetimsiz ve güvensiz olması DAC erişim denetiminin sakıncalarındandır[5].

2.3.2 MAC (Mandatory Access Control - Zorunlu Erişim Denetimi)

MAC merkezi bir yetkili tarafından belirlenen erişim kontrolü politikasını kullanarak kaynaklara erişimi kısıtlar. Sistemdeki merkezi yetkili özne ve kaynakları belli güvenlik seviyelerine göre sınıflandırmakla sorumludur. Kaynaklar gerekli kaynağa

erişim için oluşturulmuş güvenlik seviyelerine atanmaktadır. Aynı erişim seviyesine sahip veya daha üstün erişim seviyesinde olan özneler kaynağa erişebilmektedir[12].

MAC ile hiyerarşik kontrol yapısına göre erişim gerçekleşmektedir. Genellikle savunma sektöründe kullanılmaktadır [13]. Kullanıcılar kendi güvenlik seviyelerinden aşağıdaki bir güvenlik seviyesine sahip kaynaklar için yazma yetkisine sahip iken, kendi güvenlik seviyeleri üstü için sadece okuma yetkisine sahiptir[14].

2.3.3 ABAC (Attribute Based Access Control - Öznitelik Tabanlı Erişim Denetimi)

ABAC, sistem tarafından bir istek tarafından sunulmadan önce öznenin bilinemediği dağıtık sistemler için tasarlanmıştır. ABAC, özne ve kaynağın özelliklerini yani özniteliklerini baz alarak kanyaklara erişim hakkını verir veya kaynaklara erişimi reddeder[12]. ABAC modeli özne, nesne ve onların özniteliklerini baz alarak MAC ve DAC gereksinimlerinin ikisini de karşılamaktadır. ABAC modelinde 3 tip öznitelik önemlidir:

Özne Öznitelikleri: Her özne kaynak üzerinde eylem yapabilen bir varlıktır. Her özne, öznenin kimlik ve karakteristik bilgilerini oluşturan özniteliklerle bağlamlandırılır.
Kaynak Öznitelikleri: Kaynak, bir özne tarafından üzerinde eylem yapılabilen, bir varlıktır. Web servisleri, veri yapıları, sistem araçları bir kaynak olabilir
Çevre Öznitelikleri: Çevre öznitelikleri veri erişimi esnasında operasyonel, teknik oluşumlar olarak tanımlanabilir. [15].

2.3.4 RBAC (Role Based Access Control - Rol Tabanlı Erişim Denetimi)

RBAC belli bir gruba ait kullanıcıların rolleri doğrultusunda yani ortak sorumluluğa ve ya göreve sahip oluşlarına göre kaynağa erişimi sınırlandırmaktadır. Kullanıcılara uygun roller atandıktan sonra aynı kaynağa erişim farklı rollere sahip kullanıcılar tarafından sağlanabilmektedir[16] . Her rolün bir veya birden fazla işlem yapma hakkı olabilir. 3 temel kural geçerlidir:

Rol ataması: Her özne sadece kendisine atanan rol ya da roller doğrultusunda işlem yapabilir.
Rol yetkilendirmesi: Öznenin aktif rolü özne için yetkilendirilmiş olmalıdır.
İşlem Yetkilendirmesi: Öznenin aktif rolüne ilişkilendirilmiş işlem yetkisi doğrultusunda ancak özne işlem yapabilir[17].

Örneğin, insan kaynakları sistemi düşünüldüğünde insan kaynakları verilerine erişebilecek roller, insan kaynakları departmanında çalışan uzman ve yetkililer, organizasyondaki tüm çalışanlar, iş başvurusunda bulunan adaylar düşünülebilir. Eğer kullanıcı İK Uzmanı rolündeyse kullanıcı çalışanların özlük, eğitim, sertifika, kimlik gibi bilgilerine erişebilir. Kullanıcı tüm çalışanlar rolündeyse bu çalışanlar sadece kendi bilgilerini görebilir, yetkili olmadıkları için başka çalışanların bilgilerine erişemezler.

2.3.5 OBAC (Ontology Based Access Control-Ontoloji Tabanlı Erişim Denetimi)

OBAC kaynaklara erişim denetimi ve bu kaynaklara erişecek öznenin bilgilerinin ontoloji dillerinden faydalanarak sistem davranış biçiminin belirtildiği erişim denetim düzeneğidir[5]. OBAC modeli anlamsal web tabanlı bir yaklaşımla kaynağa erişim denetimi sağlamaktadır. Politikalar, kaynak ve nesne üst verisi tabanlı oluşturulmaktadır. Politikaların bir parçası olan üçlüler kaynağa erişecek olan varlık olarak özne, kaynağın kendisi olarak nesne ve politika objeleri olarak yüklemi temsil etmektedir.

OBAC' da politika nesneleri (deontik nesneler) aşağıdaki gibidir.

- İzin: Varlığın yapabileceğidir.
- Yasak: Varlığın yapamayacağıdır.
- Zorunluluk: Varlığın yapması gerekendir.
- Özel İzin: Varlığın belli bir süre içinde yapabileceğidir [18].

Anlamsal web servislerinin ontoloji tabanlı erişim denetimini için yapılan bir çalışmada, ontolojinin kullanımı erişim denetimi karar alma mekanizması için muhakeme yeteneği sağlamakta ve erişim denetim bilgilerinin otomatik olarak aranması, sorgulanması ve bulunmasına izin vermektedir [19].

2.3.6 ROWLBAC (Rol Temsil Tabanlı OWL Erişim Denetimi)

Erişim kontrolünde son yıllarda yeni politika dilleri oluşturulmuştur. XACML bu dillerden biridir[20]. XACML(eXtensible Access Control Markup Language - Genişletilebilir Erişim Denetimi İşaretleme Dili) bir erişim denetimi politika dilidir. Kullanıcılar yani özneler ve kaynaklar için istek yani eylemleri tanımlamak için XML dilinde sözdizimi sağlamaktadır. [21]. Yeni politika dilleri Ponder gibi uygulamada daha pratik diller de akademik çalışmalar sonucunda geliştirilmiş aynı zamanda kuramsal olarak anlamsal web tabanlı Rei ve KaoS dilleri üzerinde de çalışmalar yapılmıştır[20]. Ponder genel güvenlik politikalarını içermektedir. Güvenlik ve yönetim politikaları için nesne yönelimli bir dildir. Rei yetki, yasak, zorunluluk, özel izin gibi politika kurallarını kapsamaktadır ve bu politikaların eylem, kısıt ve politika objelerine ayrılmasına izin vermektedir. [22].

ROWLBAC (RBAC in OWL) erişim politikasında OWL web ontoloji dili ile RBAC (Rol bazlı erişim denetimi) bir arada kullanılmaktadır. RBAC de geçen özne, eylem ve obje gibi ana tanımlar OWL diliyle modellenmektedir. [21].

OWL (Web Ontology Language – Web Ontoloji Dili) www (world wide web) üzerinde ontolojilerin paylaşımı, yayınlanması için kullanılan anlamsal işaretleme dilidir. RDF (Resource Description Framework – Kaynak Tanımlama Çerçevesi) sözlüğünün genişletilmişidir ve DAML+OIL web ontoloji dilinden türemiştir[23].

ROWLBAC kuralları SWRL (Semantic Web Rule Language - Anlamsal web Kural Dili) ya da N3(Notation 3) dilinde belirtilebilir. ROWLBAC sadece yetkilendirme politikasını desteklemektedir[24].

3 Önerilen Mimari Yapı

3.1 Uygulama Senaryosu

Uygulama için yapılan senaryoda kurum bünyesinde İK bölümünde çalışanlar, tüm departmanlar dahil tüm çalışanlar ve kurum dışı olup kurumda çalışmaya adaylar ve bu rollere verilen yetkilerin durumu düşünülmüştür.

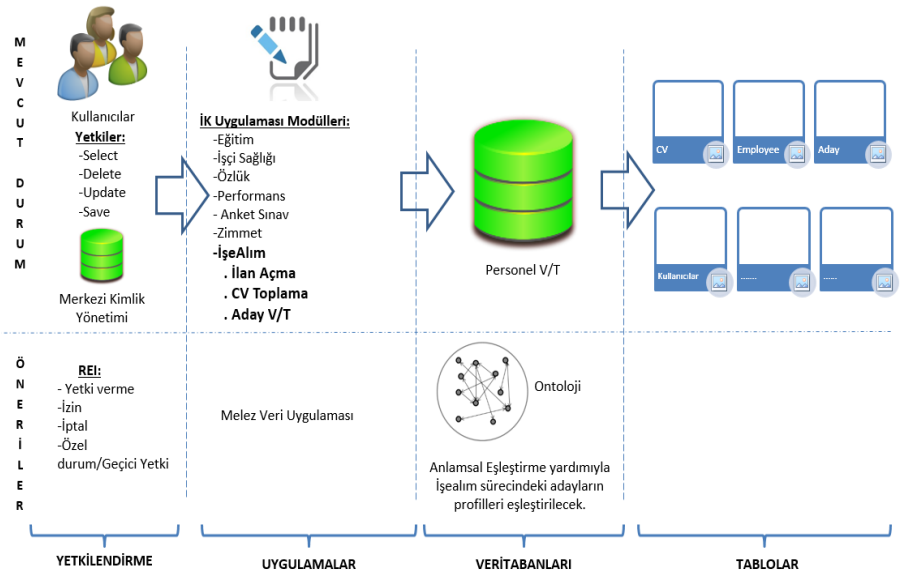
Yetkilendirme politikası örneği olarak: " İnsan Kaynakları Uzmanı, çalışanların özlük bilgilerini kendi çalışma istasyonu bilgisayarından erişebilir. "
Kısıtlama politikası örneği olarak: " İnsan Kaynakları Uzmanı 2 aylık çalışma süresi dolmadan çalışanların performans bilgilerini kendi çalışma istasyonu bilgisayarından erişemez. "

İK uygulaması içinde çalışanların bilgilerinin tutulduğu, eğitim tanımlarının yapıldığı, işealım ilan açma ve aday özgeçmiş havuzunun incelenebildiği ayrı modüller bulunabilir. Uygulama senaryosu ile ilgili olarak mevcut sistemde kullanıcıların İK uygulaması modüllerine okuma, silme, güncelleme ve kaydetme yetkileri merkezi bir bir yönetim sistemi ile verilmektedir. Böylelikle çalışanların bilgisinin tutulduğu veritabanı alanlarının yetki sistemi ile güvenliği sağlanmaktadır. Örneğin, işe yeni başlayan İK uzmanları, deneme süreleri boyunca, diğer çalışanların bilgilerini sadece görüntüleme ve listeleme hakkına sahip olabilir. İK Uygulaması modülündeki her ekran görüntüsü için listeleme, yeni kayıt, güncelleme ve silme hakkı kullanıcılara verilebilir. Verilen hak ve yetkiye göre veritabanında ilgili tablolarda değişiklikler yapılır.

İK uygulaması içerisinde ise işealım süreçlerinde doğru adayın işealımının gerçekleştirilmesi önemlidir. Kurumlarda kadro eksiklikleri sebebiyle, işalım ilanı açılır. Açık olan kadro için açılan ilana adaylar başvuru yapar. Doğru aday işe alınmadığında, çalışana verilen eğitimlerin, çalışanın süreç içinde işi öğrenmesi için yapılan çalışmaların, yeni bir aday arama işlemiyle tekrar edilmesi durumundan dolayı maliyet artmaktadır. Başarılı bir işealım süreci ile, kurum içi çalışan devir hızı düşer. Kurum içi işealım devir hızının düşmesi ise, maliyetlerin azalması demektir. Sistemde adaylar, işe başlama potansiyeli olan kişiler anlamına gelmektedir. Sistemdeki bir diğer rol ise, adayların işealımını gerçekleştirecek İK bölümü çalışanlarıdır. İK bölümü çalışanları biriken özgeçmiş havuzu içerisinden doğru adayı bulup işe alma işlemini gerçekleştirebilmelidir.

Ontolojilerle hangi kişilerin hangi kadrolara uygun olup olmadığı aday-kadro eşlemesi ile yapılabilir. Açık olan kadro için çıkılan ilana uygun adayların sistemdeki biriken özgeçmiş havuzu içerisinden eşlemesinin yapılması işleminde ontoloji çatısı kullanılabilir. Yapılan profil eşleştirmesi ile doğru adayların işealımı sağlanabilir. Profil eşleştirmesi ile kadronun gerektirdiği eğitim, askerlik, sertifika, sınav, iş tecrübesi, kişisel özellikler gibi kriterler adayların özgeçmişleri üzerinde otomatik olarak karşılaştırılarak sistemde işealım için önerilebilir. İlişkisel veritabanında tutulan işealım süreci ile ilgili kayıtların oluşturulan bu ontoloji çatısı ile anlaşabildiği OBAC ve RBAC'in bir araya geldiği mimari ile İK uygulaması için melez bir mimari

ortaya çıkmaktadır. Böylelikle sadece OBAC ya da sadece RBAC'in sınırlı olan özellikleri bir araya gelerek daha güçlü bir mimari ortaya çıkmaktadır. Ortaya çıkan melez mimarinin erişim denetimi ve güvenliği HAC ile çözümlenmektedir. Senaryo dahilinde önerilen HAC yapısı Şekil-1'de görülmektedir.



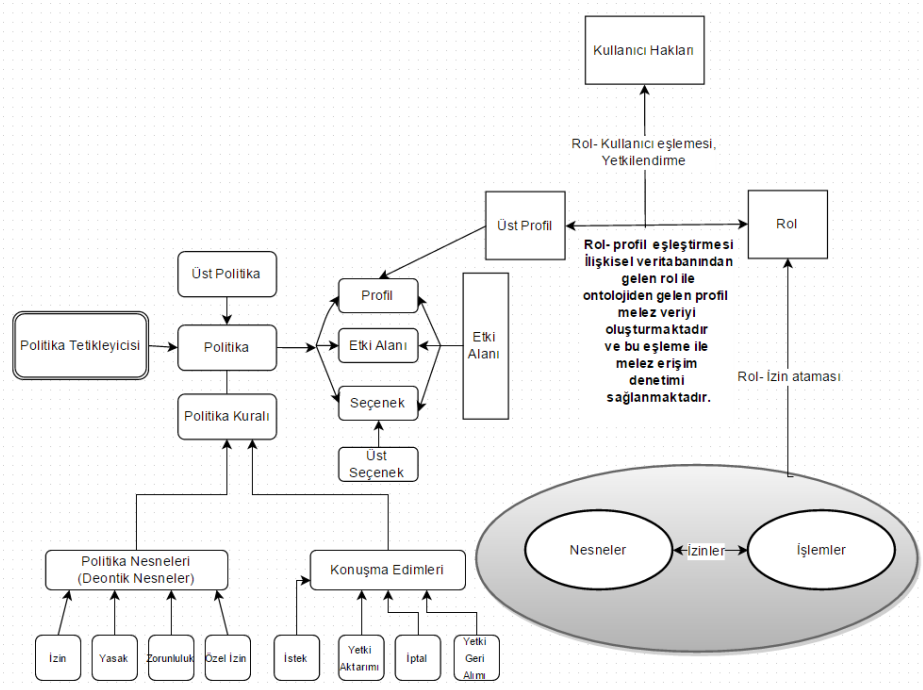
Şekil 1: Senaryo dahilinde önerilen HAC yapısı.

3.2 Önerilen Mimari

Bu bölümde, çalışma kapsamında geliştirilen RBAC ve OBAC'in karışımından oluşan melez model ve bu modelin geliştirmesi için gerekli olan araçların bilgileri tanıtılmaktadır.

Şekil-2'de önerilen melez mimarinin ilk fazı gösterilmektedir. RBAC'de ilişkisel veritabanı ile bağlantı kurularak rol- yetki ve kullanıcı- yetki atamaları, rol seviyesinde ontolojide bulunan profille eşleştirilmektedir. Böylelikle rol- profil eşleştirmesi sağlandıktan sonra kullanıcılar, sadece RBAC'deki statik rolleri değil OBAC'deki dinamik profile ait yetkilere de sahip olacaklardır.

Her iki erişim denetimi politikasının melez bir şekilde bir araya getirilmesi ile kullanıcıların yetkileri, RBAC'den gelen izin ve yasak politika nesnelerine OBAC'den gelen zorunluluk ve özel izin politika nesnelerini ekleyerek genişletilmiş olacaktır. Aynı zamanda OBAC ile istek, yetki aktarımı, iptal ve yetki geri alma, konuşma edimlerine sahip olunulacaktır.



Şekil 2 : RBAC ve OBAC melez modeli [25], [26]

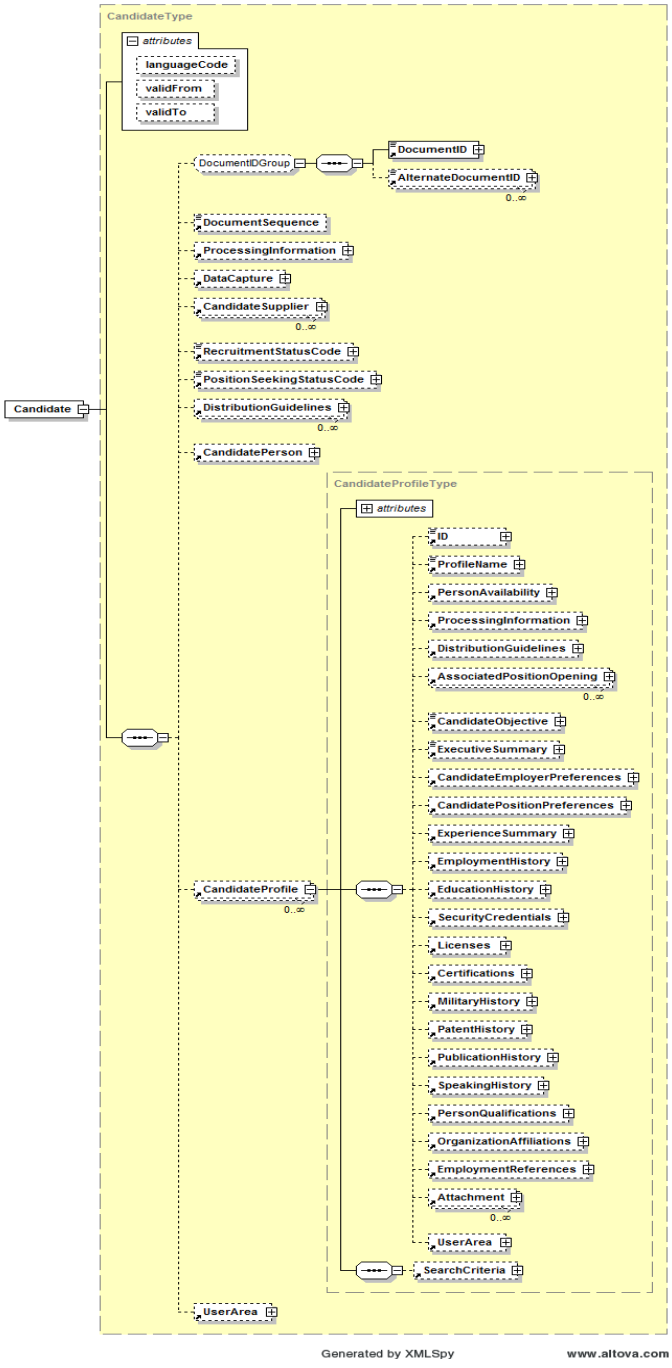
Kullanılacak metod ve yöntemler aşağıda belirtilmiştir.

OWL (Web Ontoloji Dili) : OWL ontolojileri tanımlamak için kullanılan bir anlamsal web dilidir. RDFS, DAML+OWL, OWL anlamsal web dilleri içinden bu çalışmada OWL kullanılmaktadır.Çalışmada kullanılacak İK-işealım ontolojisinde aday rolünden örnek verilecek olursa aşağıdaki şekilde işealım ontolojisi incelenebilir.

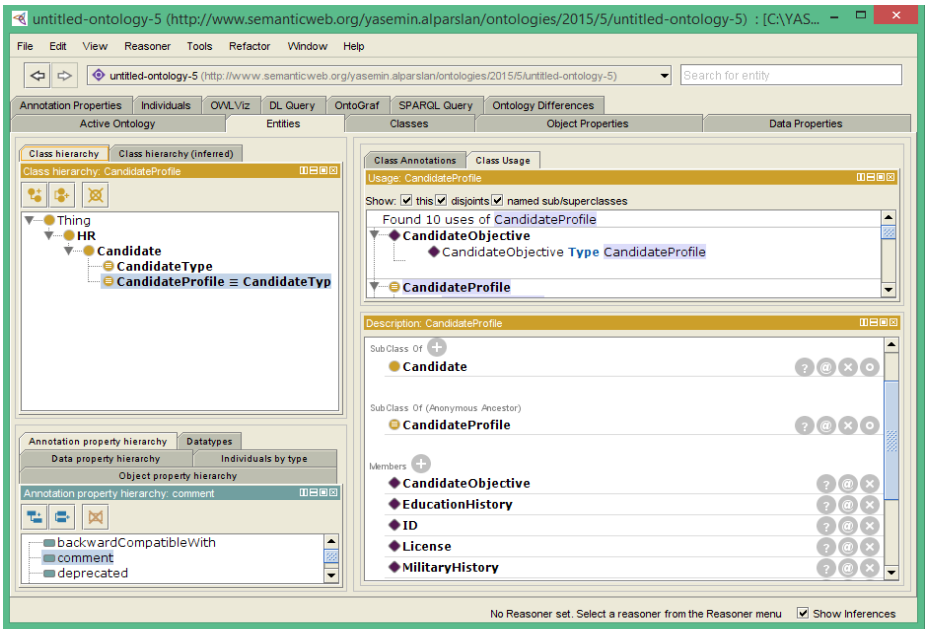
Protégé : Bir ontoloji geliştirme editörüdür. Apollo, OntoStudio, Swoop, TopBraid, gibi editörlerin arasından bu çalışmada Protégé kullanılmaktadır. Protégé kullanılmasının sebebi, grafiksel arayüz olarak kullanım kolaylığının olması, açık kaynak kod uygulaması olmasıdır.

İK- İşealım ontolojisinden bir kesit almak gerekirse, Protégé'in kullanıcı dostu arayüzü ile aşağıdaki gibi örnek bir sınıf hiyerarşisi oluşturulmuştur.

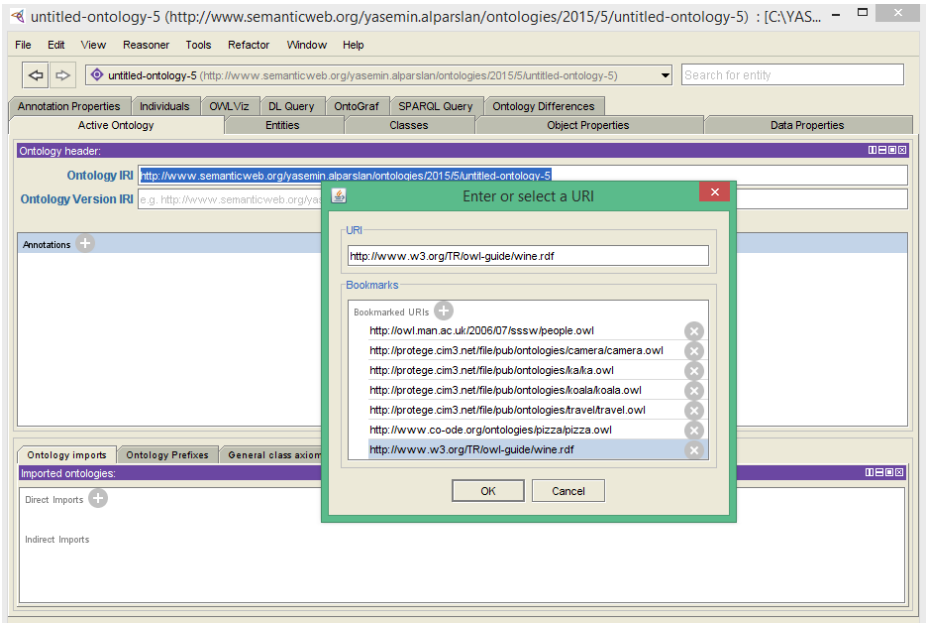
Protégé, Java tabanlı ücretsiz, açık kaynak kodlu, dosya ve veritabanı seviyesinde ontolojiyi saklama özelliği ve grafiksel arayüzü ile kullanımının kolaylığı ve hızlılığı açısından tercih edilmektedir. Proje kapsamında Şekil-3'tekine benzer bir ontoloji Protégé ile geliştirilecektir.



Şekil 3 : Aday XML şeması örneği [27]



Şekil 4 : Protege'de aday sınıfı örneği



Şekil 5 :Protege'de URI seçimi

Örneğin, varsa diğer iki ontolojiyi birleştirmek için, yani melez veri üretmek için Protégé'deki "SameAs" yapısı kullanılacaktır. "SameAs" özelliği iki sınıf örneğinin (Protégé uygulamasında individuals terimlerine karşılık gelmektedir.) birbirine eş olduğunu göstermek için kullanılır. Bir diğer deyişle iki URI referansının aynı şey olduğunu göstermektedir.

Oracle 12c : Şekil-1 deki melez veri uygulaması için yapılan mimari önerisinde kullanılacak İK ontolojilerin saklanması için Oracle 12c kullanılabilir. İlişkisel anlamda tutulan veritabanı ile OWL dilinde tutulan ontolojilerin bir araya gelmesiyle oluşan verinin saklanmasında Oracle 12c ile veri analizi ve saklanması için ileri seviyede RDF anlamsal grafiklerinden faydalanılabilecektir. Oracle veritabanı RDFS++, OWLSIF, OWL 2 RL ve OWLPrime kütüphanelerini desteklemektedir. [28]

OWL yeteneklerinden aşağıdaki maddeler desteklenmektedir:

- Sınıf, altsınıf, özellik, alt özellik, çalışma alanı,
- Özelliklerin karakteristik özellikleri: geçişlilik, smetrik, fonksiyonel, ters fonsiyonel,
- Sınıf karşılaştırmaları: eşitlik, ayrılık
- Özellik karşılaştırmaları: eşitlik
- Individual karşılaştırmaları: aynı, farklı

*Apache Jena :*Jena, Java programlama dili kullanan bir programlama aracıdır. Jena Java programları yazılırken kullanılmaktadır. Jena, RDF ve OWL dilinde yapılan tanımlamaların Java koduyla yazılmasına yardımcı olan bir araçtır. Java geliştirme seçeneği olarak Eclipse ile beraber kullanılabilir.

Jena, hangi ontoloji dili kullanıldığından bağımsız ontoloji uygulamaları geliştirmeleri için uygun programlama arayüzü sağlamayı amaçlamaktadır. Jena Ontoloji API ile OWL sınıfları veya RDFS sınıfları gösterilebilir. Farklı gösterimler için her bir ontoloji dilinde, sınıf ve özelliklerin listelendiği profil tanımları olmalıdır. Profil, Jena'nın Model sınıfının daha genişletilmiş verisyonu olan ontoloji modeline bağlanır. Model rdf verisindeki ifadelere erişmeye izin verir. Jena içerisinden ontoloji ile çalışırken RDF üçlüleri olarak kodlanan duurm bilgileri RDF modellerin içerisinde saklanır. Ontoloji API, ontolojilerin RDF sunumunda bir değişiklik yapmaz, daha kolay program yazabilmek için sınıf ve metod kümeleri eklenebilmesini sağlar.[29]

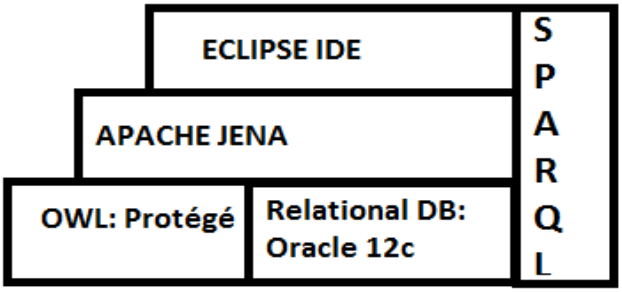
SPARQL : Bir sorgu dili olarak ontoloji de tutulan bilgilerin sorgulanması için veri odaklı çalışmaktadır. Yeni veriler yaratmak ve varolan verileri güncellemek için kullanılabilir. İşte bu noktada yaratılacak veriler melez-veri olmaktadır.Çalışmada yetki sorgulama için SPARQL kullanılacaktır.

ECLIPSE IDE JUNO : Eclipse üzerine proje geliştirirken Jena kütüphaneleri proje içine eklenecektir. Ontolojilere yeni nesneler eklemek ve varolan nesneleri sorgulayıp güncellemek için kurulmuş olan SPARQL sorgularını çalıştırmak amacıyla da kullanılacaktır. Eclipse ile Java dili kullanarak proje geliştirmek için Eclipse IDE sürümü olan Eclipse Juno kullanılabilir.

4 Sonuç ve Öneriler

Çalışma kapsamında ilk defa olarak Melez Veri ile veritabanlarındaki verilere erişim konusuna bir yaklaşım getirilmeye çalışılmıştır. Bu kapsamda, kurum için merkezi bir üst ontoloji geliştirilmesi planlanmıştır. Bu ontoloji, melez veri modelinin tabanını oluşturmaktadır. Melez veri ontolojisi kapsamında, mevcut kurum içi işleyişte anlam teşkil eden her kavram (işlev, rol,iş nesnesi) tanıtılabilecektir. Yine çalışma kapsamında, ayrıntılı olarak anlatılan yazılım altyapısı, uygulama ile birlikte geliştirilecektir.

Uygulamada önerilen mimaride kullanılacak araçlar Şekil-6'da gösterilmektedir. Melez veri olarak Oracle 12c'de tutulan ilişkisel veritabanındaki bilgiler aynı zamanda Oracle 12c'nin anlamsal web desteği ile OWL ontoloji dilini desteklemesi ile yönetilmiş olacaktır. Ontoloji tarafında kullanılacak OBAC erişim çerçevesi için gerekli sorgular SPARQL sorgulama dili ile alınacaktır. APACHE JENA ile OWL ontoloji dili ile oluşturulmuş veriler ile ilgili kod yazılabilecektir. Aracın geliştirmesinde Eclipse kullanılırken Jena projesi oluşturularak, melez veri yönetimi Java programlama dilinde sağlanmış olacaktır.



Şekil 6 : Mimaride kullanılacak araçlar

Bu kapsamda yapılan çalışmalar ile ilgili ileride çalışmak isteyenlere bir öneri olarak, söz konusu çalışmaların, gelecekte bir ileri uygulaması olarak, NoSQL kullanarak da benzer yapılar geliştirilebilir.

Kaynaklar

1. Gómez-Pérez, Asunción, Jaime Ramírez, and Boris Villazón-Terrazas. "An Ontology for Modelling Human Resources Management based on Standards." Knowledge-Based Intelligent Information and Engineering Systems. Springer Berlin Heidelberg, 2007.

2. Dorn, Jürgen, Tabbasum Naz, and Markus Pichlmair. "Ontology Development for Human Resource Management." Proceedings of the 4th International Conference on Knowledge Managements. 2007.
3. http://www.hropenstandards.org [Erişim Tarihi:20 Mayıs 2015]
4. Berners-Lee, Tim, James Hendler, and Ora Lassila. "The Semantic Web.", Scientific American 284.5 (2001): 28-37.
5. Can, Ö., Ünalır M.O., "Ontoloji Tabanlı Erişim Denetimi."Pamukkale University Journal of Engineering Sciences 16.2 (2010).
6. Ferraiolo, David F., and D. Richard Kuhn. "Role-based access controls." arXiv preprint arXiv:0903.2171 (2009).
7. Maniu, George, and Ionela Maniu. "A human resource ontology for recruitment process." Review of General Management 2 (2009): 12-18.
8. Pernici, Barbara, Paolo Locatelli, and Clementina Marinoni. "The eCCO system: an eCompetence management tool based on semantic networks." On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. Springer Berlin Heidelberg, 2006.
9. IEEE 1484.20.1/Draft 3, Draft Standard for Learning Technology – Standard for Reusable Competency Definitions, Learning Technology Standards Committee of the IEEE Computer Society (08 March 2006)
10. Dittmann, L., and Stephan Zelewski. "Ontology-based skills management."Proc. of the 8th World Multi-conference on Systemics, Cybernetics and Informatics (SCI 2004). Vol. 4. 2004.
11. Mochol, Malgorzata, Elena Paslaru, and Bontas Simperl. "Practical guidelines for building semantic erecruitment applications." International Conference on Knowledge Management, Special Track: Advanced Semantic Technologies (AST'06). 2006.
12. Kirrane, Sabrina. Linked Data with Access Control. Diss. National University of Ireland, Galway, 2015.
13. Campbell, R. H.; Liu, Z.; Mickunas, M. D.; Naldurg, P.; Yi, S., Seraphim: Building Dynamic Interoperable Security Architecture For Active Networks, Open Architectures and Network Architectures and Network Programming, 2000 (OPENARCH 2000), 2000, pp55–64
14. Samarati, P.; Jajodia, S., Data Security, from Webster, J.G., Wiley Encyclopedia of Electrical and Electronics Engineering, John Wiley & Sons, 1999
15. Yuan, Eric, and Jin Tong. "Attributed based access control (ABAC) for web services." Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on. IEEE, 2005.
16. Sandhu, R. S., 1998. Role-based access control. Advances in Computers, Elsevier 46, 237 – 286. URL http://www.sciencedirect.com/science/article/pii/S0065245808602065
17. Sandhu, Ravi, David Ferraiolo, and Richard Kuhn. "The NIST model for role-based access control: towards a unified standard." ACM workshop on Role-based access control. Vol. 2000. 2000.
18. Can, Ö., Bursa, O., Ünalır M.O., "Personalizable Ontology Based Access Control." Gazi University Journal of Science 23.4 (2010): 465-474.
19. Mohammad, A., et al. "Ontology–Based Access Control Model for Semantic Web Services." Journal of Information and Computing Science 6.3 (2011): 177-194.
20. Finin, Tim, et al. "Using owl to model role based access control." Organization (2008): 1-25.
21. Lorch, Markus, Dennis Kafura, and Sumit Shah. "An XACML-based policy management and authorization service for globus resources." Proceedings of the 4th International Workshop on Grid Computing. IEEE Computer Society, 2003.
22. Kagal, Lalana. "Rei." (2002).
23. Dean, Mike, et al. "OWL web ontology language reference." W3C Recommendation February 10 (2004).

24. He, Lijuan, et al. "Design of policy language expression in SIoT." Wireless and Optical Communication Conference (WOCC), 2013 22nd. IEEE, 2013.
25. Verma, Sonu, Suresh Kumar, and Manjeet Singh. "Hybrid Access Control Model in Semantic Web." International Journal of Information Technology (IJIT) 1.1 (2012).
26. Can, Ö., "Anlamsal Web için Kişiselleştirilebilir Ontoloji Tabanlı Erişim Denetimi ve Politika Yönetimi", Doktora Tezi, Ege Üniversitesi Bilgisayar Mühendisliği,2009.
27. http://www.hropenstandards.org/ [Erişim Tarihi:30 Haziran 2015]
28. https://docs.oracle.com/database/121/RDFRM/owl_concepts.htm#RDFRM623 [Erişim Tarihi:30 Haziran 2015]
29. https://docs.oracle.com/database/121/RDFRM/sem_jena.htm#RDFRM234 [Erişim Tarihi:30 Haziran 2015]