BAĞLAMA-DAYALI ROL TABANLI YETKİLENDİRMEDE SEMANTİK MODEL KULLANARAK ERİŞİM DENETİMİ VE YÖNETİMİ: SAĞLIK ALANI İÇİN BİR DURUM ÇALIŞMASI

USE OF SEMANTİC MODEL FOR ACCESS CONTROL AND MANAGEMENT IN CONTEXT-ORIENTED ROLE-BASED AUTHORIZATION: A HEALTHCARE CASE STUDY

DILMUROD VAHABDJANOV

Prof.Dr. HAYRİ SEVER
Tez Danışmanı

Hacettepe Üniversitesi
Lisansüstü Eğitim - Öğretim ve Sınav Yönetmeliğinin
Bilgisayar Mühendisliği Anabilim Dalı için Öngördüğü
DOKTORA TEZİ olarak hazırlanmıştır.

2015

DILMUROD VAHABDJANOV'un hazırladığı **"Bağlama Dayalı Rol Tabanlı Yetkilendirmede Semantik Model Kullanarak Erişim Denetimi ve Yönetimi: Sağlık Alanı için Bir Durum Çalışması"** adlı bu çalışma aşağıdaki jüri tarafından **BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Doç. Dr. Ebru AKÇAPINAR SEZER

Başkan .....

Prof.Dr. Hayri SEVER

Danışman .....

Doç. Dr. Nizami GASİLOV

Üye .....

Yrd.Doç. Dr. Erhan MENGÜŞOĞLU

Üye .....

Yrd. Doç. Dr. Kerem ERZURUMLU

Üye .....

Bu tez Hacettepe Üniversitesi Fen Bilimleri Enstitüsü tarafından **DOKTORA TEZİ** olarak onaylanmıştır.

Prof.Dr. Fatma SEVİN DÜZ

Fen Bilimleri Enstitüsü Müdürü

ETİK

Hacettepe Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

27 / 04 / 2015

DILMUROD VAHABDJANOV

ÖZET

BAĞLAMA-DAYALI ROL TABANLI YETKİLENDİRMEDE SEMANTİK MODEL KULLANARAK ERİŞİM DENETİMİ VE YÖNETİMİ: SAĞLIK ALANI İÇİN BİR DURUM ÇALIŞMASI

Dilmurod VAHABDJANOV

Doktora, Bilgisayar Mühendisliği Bölümü

Tez Danışmanı : Prof.Dr. Hayri SEVER

Nisan 2015, 120 sayfa

Günümüzün bilişim dünyasında bilgi teknolojileri (BT) ve bilgi güvenliği her açıdan çok önemli ve karmaşık bir problem haline gelmiştir. Koruma altına alınan bilgiye yetkisiz erişimin yapılabiliyor olması düşünülemez boyutta hasarlara ve sonuçlara neden olur. Bu bağlamda, erişim kontrolünü yönetebilmek için güvenli, esnek ve uygulanabilir basitlikte politika ve kuralların sağlanması, birçok güvenlik araştırmacıları ve mühendislerin nihai ana hedefleri arasında yerini almıştır.

Şu ana kadar yapılan araştırma ve çalışmalar sonucunda farklı yaklaşımlar temelinde belirli üstünlüklere sahip çeşitli erişim kontrolü modelleri önerilerek hayata geçirilmiştir. Bu çerçevede, güvenli erişim kontrol işlemlerinden en önemlisi rol-tabanlı erişim kontrol modeli olmuştur. Ayrıca bilgiye erişim süreçlerinin güvenli bir şekilde hızlandırılması amacıyla, bilgi işleme ve dağıtık bir yapıdaki paylaşım düzenekleri üzerinde farklı yeni yaklaşımlar ortaya çıkmıştır.

1990'ların başında "Yaygın Bilişim" yaklaşımı ortaya atılmıştır. Bu yaklaşımın temel amacı, zaman ve mekan bağımsız her yerden hizmet alınabilmesini sağlayacak akıllı iletişim sistemleri sayesinde yeni nesil BT uygulamaları

bütününde güvenli bir bilgi paylaşımıdır. Bilişim uygulamalarının yaygınlığının önemli yönlerinden biri de bağlama-dayalı sistemlerdir.

Bağlama-dayalı sistemlerinin ana konsepti - farklı yöndeki çevresel ortamları sezinleyerek, bağlam bilgilerine göre davranış süreçleri uyarlamasıdır.

Günümüzün modern teknolojilerinde iletişim ağları ve bilişim alt yapıları üzerinde kurularak, kullanıcıların her yerden ve her zaman bilgiye erişimi ve paylaşımı sağlayan düzenekler gibi yeni güvenlik değişimleri gereksinimi oldukça önem kazanmıştır. Bu bağlamda, uyarlanabilir servis ve akıllı sistemler üzerinden kaynak bilgileri erişiminin, etkili bir erişim kontrolü sistemi tarafından denetlenmesi ve koruma altına alınması gerekir.

Bu tez çalışması kapsamında, politika tabanlı yaklaşımlar ışığında geliştirilen bağlama-dayalı erişim kontrolü modelleri karşılaştırılmıştır. Ayrıca tez araştırmasının önemli amaçlarından biri de sağlık hizmetlerinde web üzerinden bilgi paylaşımını sağlayıp, “Bağlama-Dayalı Güvenlik” yaklaşımıyla bütünleştirilen kavramsal bir yetkilendirme modelinin tasarımı ve öneri çalışması gerçekleştirilmesidir. Böylece tanımlanan roller ve kurallara göre üretilen sabit bir güvenlik politikasına dayanan yetkilendirme modeli yerine daha da esnek ve durum değerlendirmesine göre anlamlı ve dinamik yapıdaki bir güvenlik politikası türetebilen bir yetkilendirme modelinin ortaya konması söz konusudur.

Anahtar Kelimeler: Erişim Kontrolü, Bağlama-Dayalı Yetkilendirme, Bağlam Modelleme, Durum Modelleme, Semantik Tabanlı Erişim Kontrolü, Rol-Tabanlı Erişim Kontrolü, Erişim Kontrol Politikası

ABSTRACT

USE OF SEMANTİC MODEL FOR ACCESS CONTROL AND MANAGEMENT IN CONTEXT-ORIENTED ROLE BASED AUTHORIZATION: A HEALTHCARE CASE STUDY

DILMUROD VAHABDJANOV

Doctor of Philosophy, Department of Computer Engineering

Supervison : Prof.Dr. Hayri SEVER

April 2015, 120 pages

In today's, Information Technologies (IT) World security have become a very important and complicated problem. The possibility of unauthorized access to protected knowledge results in unexpected damages and outcomes. In this context, developing secure, flexible and easy to implement rules and policies have become of high priority among security researchers and engineers.

Literature review on IT security shows that there have been research activities involving various access control models having certain superiorities based on different approaches. Among the proposed models, the most important one for secure access control operations is role-based access control model. In addition, different new approaches have been revealed on role based data processing and sharing mechanisms throughout distributed structures, the purpose being speeding up the processes of securely accessing to knowledge.

At the beginning of 90’s, pervasive computing approach have been suggested. The fundamental purpose of this approach is that it is a secure knowledge sharing capability enabling time and space independent service utilization from every point through new generation intelligent IT applications framework. One of the important aspects of pervasive computing is context-based systems.

The main concept of context-based systems is to adapt behavioral processes, through detecting environmental conditions.

In today’s modern technologies, access to and sharing knowledge from every place and every time by individual users necessitate new security requirements and this has become very important. In this context, accessing to knowledge through adaptive service and intelligent systems must be secured and controlled by an effective Access control system.

In this thesis, context-based access control models developed through policy-based approaches have been compared. Additionally one of the aims of thesis research is the design of a conceptual authorization model for medical processes and clinical applications. Proposed model uses a context-based knowledge sharing through web and “context-based security” integrated with web based knowledge sharing.

Consequently, instead of a fixed authorization model produced through defined roles and rules, a more flexible and dynamic structure based on situational evaluation is considered. This consideration produces a new authorization model reflecting the issues stipulated above.

Keywords: Access Control, Context-aware Authorization, Context Modeling, Situation Modeling, Semantic Based Access Control, RBAC, Access Control Policy

TEŞEKKÜR

Tez çalışmamda, karşılaşılan güçlüklerde yön gösterici olduğu, tezin her aşamasında değerli görüşlerini benimle paylaşarak verdiği desteği ve gösterdiği sabrı için danışmanım Sayın Prof. Dr. Hayri SEVER'e, pozitif yorumlarıyla her fırsatta motive eden ve yol gösteren Sayın Doç. Dr. Ebru SEZER'e, tez çalışmam sırasında karşılaştığım zor durumlarda bilgi birikimiyle görüş ve önerileri ile yön gösteren Sayın Yrd. Doç. Dr. Erhan MENGÜŞOĞLU ve Sayın Yrd. Doç. Dr. Kerem ERZURUMLU'ya, yoğun programlarına rağmen değerli vakitlerinden zaman ayırarak, doktora jürimde görev almayı kabul eden Sayın Doç. Dr. Nizami GASILOV'a, tez metinini ayrıntılı inceleyip kolay anlaşılır hale getirilmesinde yardım eden Sayın Esat Nadir ERYILMAZ'a, bugün bu noktada olmamı sağlayan Değerli Annem Yulduşhan VAHABDJANOV'a ve rahmetli Babam Baltabay VAHABDJANOV'a, her zaman yanımda olan ve manevi desteğini hiçbir zaman esirgemeyen sevgili eşim Feruza VAHABDJANOV'a ve çocuklarıma, ayrıca bana herhangi bir şekilde yardımları dokunan tüm hocalarıma ve arkadaşlarıma teşekkür ederim.

İÇİNDEKİLER

ÇİZELGELER

ŞEKİLLER

SİMGELER VE KISALTMALAR

AAA	Authentication, Authorization and Account
ABAC	Attribute-Based Access Control
AC	Access Control
ACL	Access Control List
ASC	Aspect-Scale-Context Information
ASCO	Australian Standard Classification of Occupations
CA	Central Authority
CAP	Context-Aware Policy
CAS	Context-Aware System
CL	Capability List
CoOL	Context Ontology Language
CoBrA	Context Broker Architecture
CAAC	Context-Aware Access Control
CONON	Context Based Ontology Model
CRBAC	Context Role Based Access Control
GRBAC	Generalized-Role-Based Access Control
GTRBAC	Generalized Temporal Role-Based Access Control
DAC	Discretionary Access Control
DRBAC	Dynamic Role-Based Access Control
IETF	Internet Engineering Task Force
KB	Knowledge Base
KH	Knowledge Handler
MAC	Mandatory Access Control
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Informatıon Standards
OrBAC	Organization Based Access Control
OWL	Web Ontology Language
PAP	Policy Administration Point
PMT	Policy Management Tool
PBM	Policy Based Management
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point

PMP	Privilege Managment Point
PR	Policy Repository
PS-RBAC	Pervasive Situatuion-Aware Role-Based Access Control
RBAC	Role Based Access Control
RDF	Resource Description Framework
RDFS	RDF Schema
SAML	Security Assertion Markup Language
SRBAC	Spatial Role-Based Access Control
ST	Spatio-Temporal Models
SWRL	Semantic Web Rule Language
TRBAC	Temporal Role-Based Access Control
UML	Unified Modeling Language
URI	Uniform Resource Identifier
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
W3C	The World Wide Web Consortium

1. GİRİŞ

Bilişim teknolojilerinin hızlı ilerlemesi ve günlük hayatımızda yaygınlaşması, ayrıca bilgiye erişim süreçlerin güvenli bir şekilde hızlandırılması amacıyla, bilgi işleme ve dağıtık bir yapıda paylaşım düzenekleri üzerinde farklı yeni yaklaşımlar ortaya çıkmıştır. 1990'lı yılların başında "Yaygın Bilişim[1]" fikri Mark Weiser tarafınca [1] önerilmiştir. Bu fikrin temel dayanağı, zaman ve mekândan bağımsız her yerden hizmet alınabilmesini sağlayacak akıllı iletişim sistemleri sayesinde yeni nesil BT uygulamaları üzerinde güvenli bir bilgi paylaşımıdır. Yaygın bilişimin önemli yönlerinden biri de bağlama-dayalı sistemlerdir.

Bağlama-dayalı sistemlerinin ana konsepti - farklı yöndeki çevresel ortamları sezinleyerek, bağlamsal bilgilere göre davranış süreçleri uyarlamasıdır. Bağlam hakkında birçok faklı tanımlar mevcuttur. Bunların içinde Dey [8] tarafından "Bir varlığın durumunu karakterize etmesi için kullanılan ve ilgilenilen açıdan bütünlük arz eden bilgi seti tanımı genel kabul gören bağlam yaklaşımı yaygındır. Burada varlık – kişi, kullanıcı ve uygulama dahil olmak üzere aralarındaki etkileşim ile ilgili nesnedir." şeklindeki bağlam tanımı yaygın olarak kullanılmaktadır. Bunun için bağlam-tabanlı sistemlerde üç temel işlevin gerçekleştirilmesi söz konusudur: (1) çevresel ortamdaki bağlamın sezinlemesi, (2) bağlamdaki herhangi bir değişiklik süreç-leri/nedenleri ve (3) bu değişikliklere olan tepki ya da yeni bağlama uyum sağlamasıdır.

Bazı kritik bağlama-dayalı sistemlerde tanımlama süreci ve mevcut bağlama tepkisi açısından başarısız işlem gerçekleştirmesi sonucu felaket durumunun oluşması sonucu ortaya çıkabilir.

Bu anlamda çok sayıda faktörün belirleyici olduğu sağlık hizmetleri bağlamında, en uygun hizmetin hasta güvenliğini en üst düzeyde gözeterek verilebilmesi, hastalar ve hastalıklarıyla ilgili bir dizi kritik veriye erişilmesini gerektirir. Hasta hakları ve meslek etiği çerçevesinde söz konusu kritik bilgilere erişim hem hizmeti aksatmayacak şekilde hızlı olmalı, hem de güvenlik

[1] Pervasive/ubiquitous computing

politikaları ve bağlamla ilgili bilgiler sonradan değerlendirilmek üzere derlenebilmelidir. Bu temel ihtiyaç mevcut tıbbi kaynaklara güvenli erişimi sağlayacak yetkilendirme mekanizmalarının geliştirilebilme gerekçesini net bir şekilde ortaya koymaktadır.

Örneğin, hasta bakım uygulaması çok kritik bir bağlama-dayalı sistemdir. Bu sistem hastanın tansiyonu, kan şekeri, ateşi, hastaya konmuş tanılar, hastaya daha önce yapılmış işlemler, hastaya yapılması gerekenler v.b. parametreler temelinde oluşacak bağlam bilgileri üzerine kurgulanmıştır. Hastaya uygulanacak klinik kılavuzlara uyum da bu çerçevede izlenebilir duruma gelecektir.

Günümüzün modern teknolojileri iletişim ağları ve bilişim alt yapıları üzerinde kurularak, kullanıcı bireylerin her yerden ve her zaman ihtiyaç duyulan bilgiye erişimi ve paylaşımı sağlayan düzenekler gibi yeni güvenlik gereksinimi oldukça önem kazanmıştır. Bu bağlamda, uyarlanır servis[2] ve akıllı sistemler üzerinden kaynak bilgilere erişimi, etkili bir erişim kontrolü sistemi tarafından korunması gerekir. Zorunlu Erişim Kontrolü (MAC), İsteğe bağlı Erişim Kontrolü (DAC) ve Rol Tabanlı Erişim Kontrolü (RBAC) gibi klasik erişim denetim modelleri geleneksel bilişim ortamları için tasarlanmış olup, yaygın ortama uyarlama ve kullanım sınırlamaları mevcuttur. Örneğin, klasik erişim denetim modelleri, kullanıcı ve ortam gibi bağlam bilgilerine göre erişim karar değerlendirmesi gerçekleşecek dinamik bir ortamla bağdaşmayan sabit niteliklere odaklı olmasıdır.

Sistemin davranışlarını etkileyen bağlam, sürekli değişen bir doğaya sahip olması nedeniyle bağlama-dayalı sistemlere dinamik bir karakter kazandırmaktadır.

Bu tez çalışmasında, politika tabanlı yaklaşımlar ışığında geliştirilen bağlama-dayalı erişim kontrolü modelleri karşılaştırılacaktır. Ayrıca tez araştırmasının önemli amaçlarından biri de sağlık hizmetlerinde web üzerinden bilgi paylaşımını sağlayıp, “Bağlama-Dayalı Güvenlik” yaklaşımıyla bütünleştirilen kavramsal bir yetkilendirme modelinin tasarımı ve öneri çalışması

[2] Adaptive services

gerçekleştirilmesidir. Böylece tanımlanan roller ve kurallara göre üretilen sabit bir güvenlik politikasına dayanan yetkilendirme modeli yerine daha da esnek ve durum değerlendirmesine göre anlamlı ve dinamik yapıdaki bir güvenlik politikası türetebilen bir yetkilendirme modelinin ortaya konması söz konusudur.

İkinci bölümde, bağlama-dayalı sistemleri ve politika tabanlı mimari konseptleri ele alınarak erişim mekanizmaları ile ilgili bilginin modellenmesi yaklaşımları incelenmiştir. Aynı zamanda geleneksel erişim kontrolü düzenekleri, dağıtık bir sistemde politika ihtiyaçlarını karşılamaya yönelik geliştirilen bağlama-dayalı yetkilendirme modellerinin veri veya bilgiye erişimin dinamik denetiminin sağlanması konusundaki karşılaştırmalı araştırma çalışmalara değinilmektedir.

Üçüncü bölümde, bu tez çalışmanın amacı ve araştırma yöntemi hakkında söz edilmiştir.

Dördüncü bölümde, Bağlama-Dayalı yetkilendirme modeli açıklanarak, bağlamsal politika ontolojisi, biçimsel tanımı ve tutarsız politika tespit etme ve çözümleme yöntemleri irdelenmiştir. Buna benzer diğer araştırmalar arasındaki farkları ile ilgili karşılaştırma çalışması sunulmuştur.

Beşinci bölümde, sağlık hizmetleri alanına ait bir senaryo üzerinde bağlama-dayalı yetkilendirme modelinin uyarlanması hakkında söz edilmiştir.

Sonuç bölümünde ise ileriye yönelik çalışmalarda incelenmesi düşünülen yaklaşımlar özetlenmektedir.

2. Kavramsal Çerçeve ve Literatür Özeti

Günümüzün bilişim dünyasında, bilgi teknolojisi ve bilgi güvenliği her açıdan çok önemli ve karmaşık bir problem haline gelmiştir. Koruma altına alınan bilgiye yetkisiz erişimin yapılabilmesi beklenmeyen boyutta hasarlara neden olur. Bu bağlamda, erişim kontrolünü yönetebilmek için güvenli, esnek ve basit politika kurallarının sağlanması, birçok güvenlik araştırmacıları ve mühendislerin nihai ana hedefidir.

Konu hakkındaki birçok araştırma, yetkisiz erişim sorunlarını azaltmaya ve çözmeye çaba harcayarak, spesifik bilgi ve verilerin korunması olmak üzere bilgi güvenliği alanlarında önemli ölçüde ilerleme kaydedilmiştir. Bilgi güvenliği disiplin kuralları yanı sıra, bilgi güvenliği kurumu “erişim kontrolü” önemli bir bilgi güvenliği sorunu olarak kabul edilmiştir. Genelde, erişim kontrol süreci kapalı bir ortamda izinsiz erişime karşı kaynakların korunması üzerinde yoğunlaşmaktadır. Kullanılan kontrol düzeneği, öncelikle kimlik tanıma ve tanınan özne nitelikleri ya da özel yetkilendirme kurallarına odaklanır [11].

Erişim kontrolü temel olarak, özne, nesne ve erişim hakları gibi bileşenlerden oluşmaktadır. Özne, nesneye erişim yeteneğine sahip aktif bir varlık yada bir süreçtir. Genelde herhangi bir kullanıcı bir uygulamaya veya nesneye bir işlem aracılığıyla erişmeye çalışır. Temel erişim kontrol sistemlerinde üç farklı özne kategorisi mevcuttur: kullanıcı, grup ve sistem dışı kullanıcı. Nesne, erişimi denetlenen herhangi bir kaynağı temsil eden pasif varlıktır. Erişim hakları, öznenin erişim sürecinde nesne üzerinde gerçekleştireceği eylemleri ifade eder. Erişim hakları – okuma, yazma, çalıştırma, silme, oluşturma ve tarama işlemlerinden oluşur.

Erişim kontrolünü tanımlamanın birçok yolu vardır. Bu anlamda, bir öznenin yetkisiz erişimlere karşı korunan bir kaynak veya nesneye erişim izni ve reddi için karar düzeneği olarak tanımlanabilir. Bu nedenle, erişim kontrolü 3 temel güvenlik bileşenine dayanır. Bu üç temel bileşene, kimlik tespiti, güvenilirlik ve inkâr edememe (Non-Repudiation) alt bileşenleri de eklenebilir.

- Gizlilik: Bilgi kaynağının yetkisi ve izni olmayan kişilerin eline geçmesinin engellenmesidir. Genelde, gizlilik ilkesinin sağlanmasında şifreleme algoritmaları kullanılır;

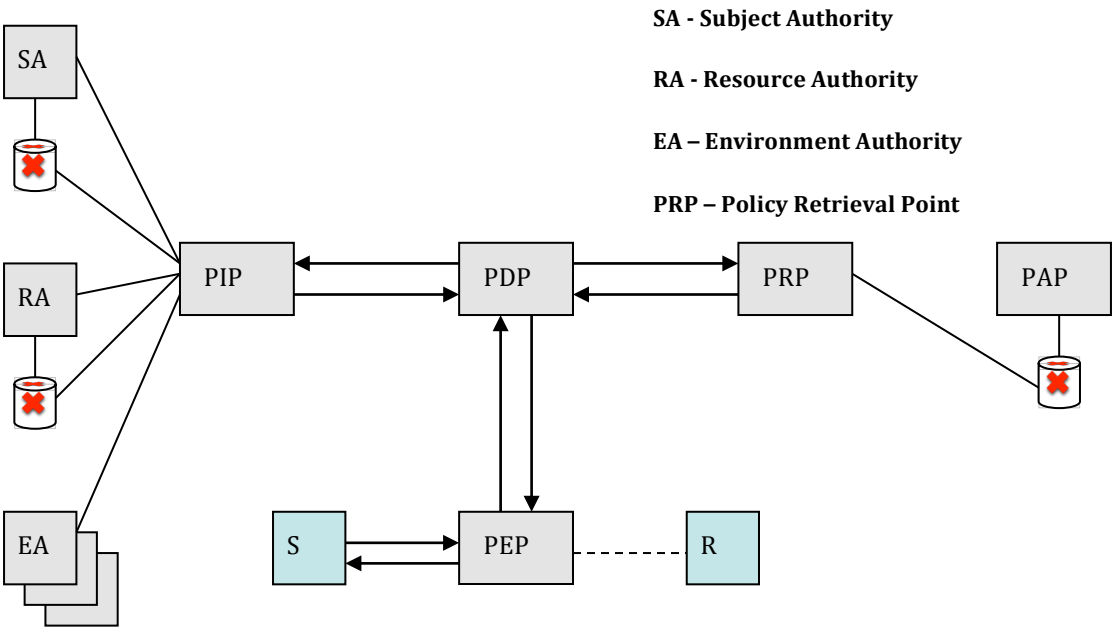
- Bütünlük: Bilgi içeriğinin belli bir kısmının ya da tamamının değiştirilmemesi bütünlük ilkesiyle sağlanır. Bilgi bütünlüğünün sağlanması için özetleme algoritmaları kullanılır;
- Erişilebilirlik: Bilgi kaynağına zamanında erişim, sistem kullanıcıları için büyük bir önem taşımaktadır. Erişilebilirlik hizmeti, kurum içi ve dışından gelebilecek tüm tehditlere karşı bilişim sistemlerini korumayı hedefler. Bunun sayesinde, kullanıcıların erişim yetkisine sahip verilere zamanında, hızlı ve güvenli bir şekilde ulaşması sağlanmaktadır.

Ayrıca bilgi güvenliği kapsamında bir erişim kontrol sisteminin sağladığı temel hizmetler, “Kimlik doğrulama”, “Yetkilendirme” ve “İzlenebilirlik” olarak ifade edilebilir.

Burada kimlik doğrulama ile sisteme hangi öznelerin giriş işlemi yapabileceği belirlenmektedir. İzlenebilirlik ile ise öznelerin sistem üzerinde gerçekleştirdiği işlemlerin veya hangi nesneye eriştiklerinin bilinmesi ve izlenmesi sağlanmaktadır. Yetkilendirme, öznelerin hangi işlemleri gerçekleştirmeye veya hangi nesnelere erişmeye yetkili olduğunu belirlemektedir. Yetkilendirme konseptleri temel olarak şöyle sıralanabilir:

- Kayan yetkilendirme (Authorization Creep) – Kişinin kurum içindeki hareketli görev değişimi sürecinde, önceki yetkilerin kaldırılmaksızın yeni erişim hakları ve yetkilerin atama işlemlerinin gerçekleşmesi;
- Sıfır varsayımı (Default to Zero) – Tüm erişim kontrol düzeneklerinin, sıfır erişim ile başlamak kavramına dayanması ve sonra bunun üzerinde yapılandırma işlemleri gerçekleştirmesi;
- Erişim kontrol listeleri (Access Control Lists - ACL): Belirli nesneye erişmek için yetkili olan öznelerin listesi. Genelde, okuma, yazma, çalıştırma, ekleme, değiştirme, silme ve yaratma gibi erişim tipleri üzerinde işlem yapılmaktadır;
- Bilinmesi gereken ilkesi (Need to Know Principle) – Kişinin görevi gereği sadece ihtiyaç duyulan bilgiye erişim verilmesi konseptine dayanmaktadır;

Genelde sistem tarafından kimliği doğrulanmış öznelerin (kullanıcıların) yetkilendirme modeli basit olarak "**Kullanıcı -> (Kaynak, İşlem)**" şeklinde tanımlanabilir. Bu modelde yetkilendirme işlemi kullanıcı ile bilgi kaynağı ve bu bilgi kaynağı üzerinde tanımlanmış işlem çiftleri arasında bir ilişki olarak tanımlanır. Burada işlem boş olduğu zaman, sadece kaynak erişimi söz konusudur. Genelde bir yetkilendirme mimarisi, özne (Subject - S) ile nesne ya da kaynak (Resource - R) arasında yetki kararlarının yürütülmesinden sorumlu "Politika Yürütme" (Policy Enforcement Point - PEP), güvenlik politikaları bilgi kümesi üzerine işlem gerçekleştiren politika bilgi noktası (Policy Information Point - PIP), politika yönetim arabirimi (Policy Administration Point - PAP), uygulanabilir politikaların değerlendirilmesinden ve yetki kararının (onay ya da red) verilmesinden sorumlu politika karar noktası (Policy Decision Point - PDP) gibi ana bileşenlerden oluşmaktadır (Şekil 2.1).



Şekil 2.1 Yetkilendirme Mimarisi [85]

Yetkilendirme modeli üç temel varsayım üzerine dayanır:

- En az yetki – Kullanıcıya sadece gerekli olan en alt seviye yetki verilir;
- Güvenli sistem –sadece kullanıcı ile arasında tanımlanan ilişki varsa (Kaynak, İşlem) çiftine yetkilendirme geçerlidir. Aksi yönde yetkilendirme söz konusu değildir;

- Yetkilendirme bilinci – Yetkilendirme gereksinimleri için bilinçli bir modeli kullanır.

Sonuç olarak da, erişim kontrolü belli bir varlığa sadece yetkili özne veya süreçlerin tanımlanan hakları temelinde erişilebilmesini sağlamaktadır. Bu bağlamda, üç ana geleneksel erişim kontrol modeli mevcuttur:

1. İsteğe bağlı Erişim Kontrolü (Discretionary Access Control - DAC)
2. Zorunlu Erişim Kontrolü (Mandatory Access Control - MAC)
3. Rol Tabanlı Erişim Kontrolü (Role Based Access Control - RBAC)

Bu modeller, "özne", "nesne" ve "işlem" bileşenlerinden oluşan yetkilendirme kurallar kümesi temelinde geliştirilmiştir. Basitçe tanımlanırsa, bir kullanıcının (özne) belirli bir kaynağa (nesneye) erişme yetkisi olup olmadığını ve kullanıcının erişim izni olan kaynak üzerinde gerçekleştirebileceği işlemi ifade eder[16]. Geleneksel erişim kontrolü modellerinin ana konsepti, kapalı bir güvenlik ortamındaki bilgi kaynaklarının korunmasıdır. Ancak bilişim sistemlerin hızlı gelişim sürecinde, yeni güvenlik gereksinimlerine ihtiyaç duyulmakta ve dolaysıyla daha da sağlam yeni bir güvenlik düzeneklerinin geliştirilmesi söz konusudur [13].

Geleneksel güvenlik modelleri, dağıtık bir ortamda paylaşılan bilgi kaynaklarına yetkisiz erişim sorunlarına yeterli düzeyde çözüm getirmemektedir. Bu çerçevede bilgi kaynağına yetkisiz erişime karşı korunabilmek için daha da sağlam ve esnek modellere ihtiyaç duyulmaktadır. DAC modeli, esasen nesnelere erişimin kontrol edilmesini sağlar. Bu model, bilgi akışı denetimini yapmaz. MAC ise bilgi akışı sürecini kontrol eder, ancak nesnelere erişimi kontrol etmek için uygun olmayabilir. RBAC, bilgi kaynaklarına erişim kontrolünü ve yönetimi sağlamakta ve kurumsal alanları denetlemektedir. Ancak yaygın bilişimde veya dağıtık açık bir sisteminde bilinmeyen öznelerin bilgiye erişiminin kontrolünde yeterli değildir.

Bilgi güvenliğinin sağlanmasında büyük öneme sahip olan erişim kontrolleri uygulama öncelikleri arasında yer almasına rağmen, bu kadar çok bulguyla ilişkilendirilmesi sebebiyle hızla artmakta olan ve oldukça karmaşık bir yapıya sahip olan sistemler üzerinde geleneksel erişim kontrolü tipleriyle mevcut beklentileri karşılayamaz ve uygulanamaz hale gelmiştir.

Sonuç olarak, Zorunlu Erişim Kontrolü (MAC), İsteğe bağlı Erişim Kontrolü (DAC) ve Rol Tabanlı Erişim Kontrolü (RBAC) gibi klasik erişim denetim modelleri geleneksel bilişim ortamları için tasarlanmış olup, yaygın ortama uyarlamada kullanım sınırlamaları mevcuttur.

Sistemin davranışlarını etkileyen bağlam sürekli değişen bir doğaya sahip olması nedeniyle bağlama-dayalı sistemlere dinamik bir yapı kazandırmaktadır. Böyle bir güvenlik yaklaşımı, kullanıcının paylaşılan bilgiye her zaman ve her yerden erişebilmesini sağlar.

2.1 Bağlama-Dayalı Sistemlere Genel Bakış

Bağlama-dayalı sistemler, ilk defa 1994 tarihinde Schilit ve Theimer [26] tarafından ele alınarak, "özne ve nesne kümelerinin kullanım yeri veya ortamına (bağlam bilgileri) göre değişim sürecinde etkileşimli uyarlanan" sistemler hakkında yorumlar ortaya sunulmuştur. 1992'de yapılan "Olivetti Active Barge" [27] çalışması, bağlama-dayalı sistemler ile ilgili ilk araştırma çalışmasıdır.

Bağlama-dayalı kavramsal bir terimine olmasının yanısıra adaptif [18], tepkin (reactive) [19], yanıtsal (responsive) [21], durumsal [23], bağlama-duyarlı [24] ve çevresel ortama dayalı [22] gibi diğer terimler ortaya çıkmıştır. Bağlam kullanmanın ana nedenleri hakkında bazı yorum ve tanımlamalar da yapılmıştır. Örneğin, Dey [20] bağlama-dayalı sistemi, kullanıcı bağlam bilgisi doğrultusunda adaptasyon işlemini gerçekleşen süreç olarak tanımlar. Salber [25] ise bağlamın eşzamanlı olarak algılanmasına dayanarak işlemi gerçekleştirme üzerinde maksimum esneklik sağlayabilen bir sistem olarak tanımlamıştır.

Birçok araştırmacı bağlama-dayalı uygulamaları tanımlarken, "uygulama alanı ve kullanıcı bağlam bilgisine dayanarak, dinamik değişim yada adaptasyon yeteneğine sahip" uygulamalar olarak ifade etmiştir. Sonuç itibariyle, bağlam kullanma temelinde kullanıcı işlemlerine bağlı olarak uygun bilgiyi ve/veya hizmetleri sağlayan sistemi, bağlama-dayalı sistem olarak adlandırır.

2.1.1 Bağlam Teriminin Tanımı

Bilgisayar bilimlerinde "bağlam" terimi: çevre, ortam, kullanıcı, uygulama alanı gibi belirli bir koşul, durum veya varlıklar için kullanılmaktadır. "Bağlam"

sözcüğü birçok araştırmacılar tarafından tanımlanmaya çalışılmıştır. [15] Araştırmacıları bağlam sözcüğünü, insan kimliği, bulunduğu yer ve nesne belirleyici nitelikler olarak yorumlamışlardır. Buna benzer olarak da [10] bazı araştırmacılar bağlamı, kullanıcı kimliği, çevre, zaman ve mekan olarak ifade etmişken, diğerleri [12] ise spesifik kullanıcı, ortam veya nesne için ilgili kavramsal ve fiziksel durum belirleyici olarak tanımlamıştır.

Dey [8] tarafından "Bir varlığın durumunu karakterize etmesi için kullanılan herhangi bir bilgi yaklaşımını ön plana çıkar. Burada varlık – kişi, kullanıcı ve uygulama dahil olmak üzere arasındaki etkileşimle ilgili nesnedir." şeklindeki bağlam tanımı bağlama-dayalı sistemler alanında yaygın kullanılmaktadır.

Bağlam aslında, yaygın sistemdeki herhangi bir elementin bir özelliğini veya niteliğini belirler. Bağlam türü ve açıklaması olduğu gibi ayrık/nominal değerlere sahiptir ve hiyerarşik yapıda sınıflandırılabilir.

Bu anlamda bağlam - ele alınan ya da göz önünde bulundurulan bir durumda, durumu net olarak tanımlamaya yarayan koşulların ve parametrelerin oluşturduğu bir "Durum Belirleyicileri" kümesidir. Bağlam, ortaya çıkan, karşılaşılan veya karşılaşılması öngörülen belli bir durumu betimleyen (tasvir eden) bir bilgiler kümesidir(İfadeler kümesi):

- Kimlik (Kim?)

- Yeri (Nerede?)

- Zaman (Ne zaman?)

- Etkinlik (Ne tür?)

Varlık ise kullanıcı ve uygulama arasındaki etkileşimi gösteren kişi, alan ya da nesne olabilir. Böylece bağlam varlığı (entity) birçok farklı bilgi tiplerini içerebilir. Bu bilgi tipleri fiziksel (kişi, bilgisayar, nesne), sanal (uygulama servisi, kullanıcılar grubu, güvenlik etiketleri) veya kavramsal (yer, mekân, zaman v.s.) olabilir.

2.1.2 Bağlam Sınıflandırılması

Tutarlı bağlam bilgileri üzerinde kurgulanarak, daha da esnek ve güvenli bir yetkilendirme sistemi tasarımında, bağlam bilgi tiplerinin doğru şekilde sınıflandırılması büyük öneme sahiptir. Ryan [46] ve Schilit [47] tarafından

yapılan çalışmalarda, mekân, çevre, kullanıcı kimliği ve zaman gibi bağlam bilgi tipleri kullanılarak, nereden, kim ve ne tür kaynak gibi önemli bağlamsal kavramları üzerinde kurgulanmıştır. Buna benzer çalışmalarından biri Chen ve David Kotz genel sınıflandırmasına göre bağlam,

- Kullanıcı Bağlamı – kullanıcı ile ilişkili bir takım bağlam bilgileri (yaşı, konumu, hastalık özgeçmişi v.s.);
- Fiziksel Bağlam – fiziksel çevre ile ilişkili bir takım bağlam bilgileri (ışık, sıcaklık derecesi, bulunduğu yer, hava durumu v.s.);
- Geçici Bağlam – zaman ile ilişkili bir takım bağlam bilgileri (gün, tarih ve mevsim v.s.);

olarak belirlenmiştir.

Bağlama-dayalı uygulamalar genelde "kim, nerede, ne zaman ve ne için" şeklindeki varlıklar temelinde işlem gerçekleştirir ve "nedeni" belirleyici durum üzerinde oluşan bilgileri kullanmaktadır.

Bu kapsamda mekân, kimlik, zaman ve eylem gibi öncelikli bağlam bilgi tipleri, belirli nitelikteki varlıkların durumunu karakterize eder. Bu bağlam türleri sadece "kim, ne, ne zaman ve nerede" gibi oluşumları cevaplandırmakla kalmayıp, diğer bağlam bilgisi kaynakları üzerindeki eylemi de belirler. Örneğin, hasta kimliği içerisinde telefon numarası, adres bilgileri, doğum tarihi, risk faktörleri, kan grubu, tansiyonu v.b. ilgili bağlamsal bilgilerden oluşmaktadır ve bunlar kısa olarak şöyle özetlenebilir:

- Yer Bilgisi (yer, yönelim, hız ve ivme);
- Zaman Bilgisi (zaman, tarih ve mevsim);
- Çevresel Bilgi (ısı derecesi, hava ve ışık veya gürültü düzeyi);
- Kaynaklar (aygıt, bilgisayar, tablet, kablosuz erişim cihazları AP);
- Fizyolojik ölçümler (tansiyon, nabız, solunum hızı, kas aktivitesi ve ses tonu);
- Eylemler (konuşma, okuma, yürüme ve koşma);

2.1.3 Bağlam Modeli

Model, bir sistemin tasarlama, geliştirilme, çalışma veya işletilme aşamalarındaki belirgin bir görünümdür. Her model belli bir üst model ile ilişkili

olup, belirgin bir üst model dili ile ifade edilir. Bağlamı aslında, işlenmesi ve depolanması gereken bir ham veri olarak da düşünülebilir. Bu anlamda, bağlamı tanımlayan ve işlenebilir bir biçim şeklinde bağlamsal bilgileri depolayan bir bağlam modeline ihtiyaç duyulmaktadır. Bu konuda yapılan temel çalışmalar [7] şöyle sıralanabilir:

I. Anahtar-Değer Modeller (Key-Value Models): "isim-Ali, zaman-17:00, mekan-hastane" şeklindeki basit bir bağlam modellemedir. Bu model, basit bir veri yapısına sahip olup, yönetim kolay olmasına rağmen, tutarlı bağlamsal bilgi alma algoritması temelinde uygun yapılanma için yetersiz kalmaktadır. Genelde işbu yaklaşım dağıtık iş akışı servisleri mimarisinde sık kullanılır.

II. İşaretleme Şema Modeller (Markup Scheme Models): Nitelikler ve içerik işaretleme etiketlerinde oluşan hiyerarşik veri yapısına sahiptir. İçerik işaretleme etiketleri ardışık olarak diğer işaretleme etiketleriyle ilişkili olarak tanımlanır.

III. Grafik Modeller (Graphical Models): Kavramsal bağlam şemasının oluşturulması için UML olarak ifade edilen Tekil Modelleme Dili kullanılmaktadır. UML, etkili bir grafik modelleme aracıdır. UML'nin jenerik yapısı bağlam modeli için elverişlidir. Böyle bir modelleme, varlıklar arası ilişkisel ER-modelini türetme olanağını da sunmaktadır. Bu ise [36] 'da bahsi geçen bilgi sistemi tabanlı bağlam yönetim mimarisindeki ilişkisel veri tabanı için yapılandırma aracı olarak çok kullanışlı bir yaklaşımdır.

IV. Nesne Yönelimli Modeller (Object Oriented Models): Bu modelleme, nesneler şeklinde ayrıştırılan bir sistemde bilginin modellenmesini sağlayan bir yöntemdir. Bu modellemede, bağımsız olarak oluşturulan nesneler bir kimlik, durum ve davranış belirler. Her nesnenin de bir tanımlayıcı/kimliği vardır. Bir nesnenin durumu, nesne özniteliklerinin aldığı değerler kümesidir. Bir nesnenin davranışı ise nesne durumu üzerinde işleyen yöntemler kümesidir. Bu modelleme, nesnelerin diğer nesnelerden bilgi ve işlemleri miras alabildiği kalıtım ve sınıf hiyerarşi özelliğini kullanarak, nesnelerin öznitelikleri ve yöntemlerini yeniden kullanma olanağını tanır. Bağlam bilgileri doğası gereği dinamik

olduğundan bağlama-dayalı sistemlerde sorun haline gelmeye başlamıştır. Bu yaklaşımın kullanılmasının ana hedefi, nesne düzeyindeki bağlam işlem ayrıntılarının çerçevelenmesi ve bağlam bilgilerine sadece belli ara yüzler aracılığıyla erişilmesidir.

V. Mantık Tabanlı Modeller (Logic-Based Model): Bu yaklaşımda bağlam tanımlamaları - ifadeler, olgular ve kurallar üzerinden yapılmaktadır. İfadeler, bir takım diziler kümesi halinde birleştirilmektedir. Genellikle mantık tabanlı bir sistemde ekleme, güncelleme ve silme işlemleri, olgular koşulları veya durumsal kuralları türeten bağlamsal bilgiler üzerinde yapılır. İlk mantık tabanlı bağlam modelleme yaklaşımı, McCarthy ve onun Stanford [38,91] ekibi tarafından araştırma çalışmaları sonucu 1993'de "Bağlamın Biçimlendirilmesi" olarak yayınlandı. McCarthy bağlamı – yapay zekâda kullanılabilecek soyut matematiksel varlıklar olarak tanımlanmıştır. Bu yaklaşımın temel ilişkisel biçimi: ist(c,p) – p önerilen koşul için c bağlam doğrudur anlamına gelmektedir. Örneğin: ist(bağlam ("Bilgisayar Mühendisliği Bölümü"), "Ahmet öğrenci"). McCarthy modeli, kalıtım konseptini destekliyor.

Diğer mantık tabanlı bağlam modellemelerinden biri de Akman ve Surav [29] tarafından önerilen "Genişletilmiş Durum Teorisi" yaklaşımıdır. Bu model, Barwise ve Perry [30] tarafından önerilen "Durum Teorisi"nin genişletilmiş bir halidir. Barwise ve Perry semantik doğal dil teorisini bir biçimsel mantık sistemi içerisine uyarlamaya çalışmıştır. Akman ve Surav ise söz konusu yaklaşımı kullanarak, durumsal türleri ile bağlam modeli kavramını uygulayarak mevcut sistemi genişletmiştir. Buna benzer olarak "Çoklu Bağlam Sistemi"(Giunchiglia [32,33]) ve "Bağlam Algılama Modeli"(Gray ve Slaber[34]) çalışmaları yapılmıştır.

VI. Ontoloji Tabanlı Modeller (Ontology Based Models): Ontoloji, kavram ve ilişkileri belirtmek için umut verici bir araçtır. Yani, kavramlar arasındaki ilişkileri formel olarak içeren bir yapıya sahiptir. Ontoloji felsefe kavramı olarak varlık bilimi ve nesnelerin birleşimi olarak anlam taşır, ayrıca varlıklar için sistematik bir açıklama sunar. Ontolojinin "kavramsallaştırmanın biçimsel ve açık şekilde ifade edilmesi" tanımı bilgisayar biliminde çok benimsenmiştir. Ontolojiler, ontoloji dillerle tanımlanarak, birçok uygulama alanı için farklı ontolojik dillerin

kullanımına zemin hazırlanmıştır. Bunlardan en sık ve yaygın kullanılanları RDF (Resource Description Framework) ve OWL (Web Ontology Language) dilleridir. RDF'de her kaynak bilgisi URI yapısına sahip olmakla beraber nesne, yüklem, özne üçlüsü temelinde anlamın ifade edilmesi sağlanmaktadır. Söz konusu üçlüler ise XML etiketleriyle ifade edilmektedir. Ayrıca RDF veri modelini genişleten RDFS (RDF-S ya da RDF/S - RDF Schema) gösterimi kullanılarak, sözcük kümesinin tanımı gerçekleştirilmektedir. Burada sözcük kümesi olarak, belli bir alanda kullanılacak nesneler ve nesneler arasındaki alt/üst küme ilişkileri, nitelikleri ve niteliklerin değerleri ifade eder. Diğer en sık kullanılan dil ise RDF'e bir eklentisi olan OWL dili olup, OWL Full, OWL-DL (Description Logic) ve OWL Lite olmak üzeri üçe ayrılır. OWL'de küme işlemleri yapılarak niteliklerin alabildiği değerler üzerinde kısıtlama işlemlerinin gerçekleştirilmesi ve eşleme ilişkileri tanımlanması sağlanmıştır. Burada nitelikler, nesne ve veri tipi olarak ikiye ayrılmıştır. OWL dili, W3C (The World Wide Web Consortium) tarafından standart bir dil olarak benimsendiği için ontolojik modellerin tasarım ve geliştirilmesinde çok yaygın kullanılmaktadır.

Bağlamsal ontoloji modelleme yaklaşımının ilklerinden biri Ötztürk ve Aamodt [39] tarafından sunulmuştur. Bu çalışmada, bağlamsal bilgileri kombinasyonu ile çeşitli kavramların geri çağrılması ve tanıma arasındaki farklılıklar üzerinde analizler gerçekleştirilmiştir. Bu araştırma sonucunda, farklı etki alanlarındaki bilgiyi normalleştirme ve birleştirme gereksinimi oluşmuştur. Ontoloji modelleme ile ilgili başka çalışmalardan biri de "Aspec-Scale-ContextInformation(ASC)" [40] modelidir. Bu yaklaşımda, ontoloji üzerinde modelin temel konsepti tanımlama işlemi standartlaştırma yoluyla sağlanarak, yaygın bilişim sisteminde bağlamsal bilginin paylaşılabilir ve kullanılabilir duruma getirilmiştir. Bu modelin uygulama sürecinde (Context Ontology Language - CoOL) bağlam ontoloji dili kullanılmıştır. CoOL dili, dağıtık bir sistemdeki çeşitli uygulamaların bağlama-dayalı niteliğinin kazandırılması amacıyla kullanılmaktadır. Wange et al. [35] tarafından önerilen CONON (Context Based Ontology Model) bağlam modellemenin ana fikri ASC/CoOL ile aynıdır. Aynı zamanda, bağlam bilgi paylaşımı ve kullanımı, mantıksal

çıkarım olanakları sunan ontoloji tabanlı bir bağlam modelidir. Burada bağlamsal varlıklar temelindeki genel özellikleri ve etki alanına özgü nesne kümeleri tespit eden üst ontoloji bilgisi oluşturulmaktadır. CONON ontoloji semantik denklem işlemleri için OWL-DL dili kullanmaktadır. Ayrıca ontoloji tabanlı bağlam modelleme konusunda umut verici bir çalışmalardan biri CoBrA (Context Broker Architecture) [31] sistemidir. Bu yaklaşımda varlıkları - kişi, mekan veya bağlamsal diğer nesneler olarak karakterize eden ontolojik konsept kümeleri üzerinde işlem yapılmaktadır. CoBrA, bağlam-dayalı sistemlerinde işlemleri gerçekleştirmeyi sağlayan bilgi aracı (broker) merkezli etmen (broker-centric agent) mimarisini kullanmaktadır.

Sonuç itibariyle, yaygın bilgisayar sistemleri ortamında bağlam modelleme yaklaşımlarının uygulanabilirliği açısından aşağıda belirtilen koşullar büyük öneme sahiptir.

1. Dağıtık bir yapı: Herhangi bir yaygın bilgisayar sisteminin doğası gereği dağıtık bilgisayar sisteminin bir türevidir. Bu anlamda, bağlam modelinin yapısı ve yönetimi, aynı zamanda veri özelliklerinin dinamik bir yapıda olması çok önemlidir.
2. Kısmi doğrulama: Modeller üzerinde hata riskinni artmasına neden olan bağlamsal ilişkilerinin karmaşıklığı açısından bağlamsal bilginin kısmen doğrulanması çok önemlidir.
3. Bilginin verimi ve kalitesi: Yaygın bilgisayar ortamında farklı sensor niteliğindeki varlıklar tarafından verimli verilerin elde edilmesi söz konusudur. Bunun da bir bağlam modelinin dağıtık bir bilgisayar sisteminde kullanılabilmesi için uygun olmalıdır.
4. Eksiklik ve belirsizlik: Dağıtık bilgisayar sisteminde uygun varlıkları temsil eden ve dağıtık bir ağ üzerinden elde edilen bağlamsal bilgiler, çoğu zaman eksik ya da tutarsız olabilmektedir. Model, tutarlı bu durumu ele alan düzenekleri kullanarak, tutarlı bağlam bilgileri elde edebilmelidir.
5. Biçimsel tanımı: Bağlamsal veri ve ilişkilerinin, net ve izlenebilir bir şekilde tanımlanması her zaman sorunludur. Bu nedenle, bağlamsal bilgi ve ilişkileri yorumlayacak biçimsel bir tanımlama dilinin kullanılması

söz konusudur.

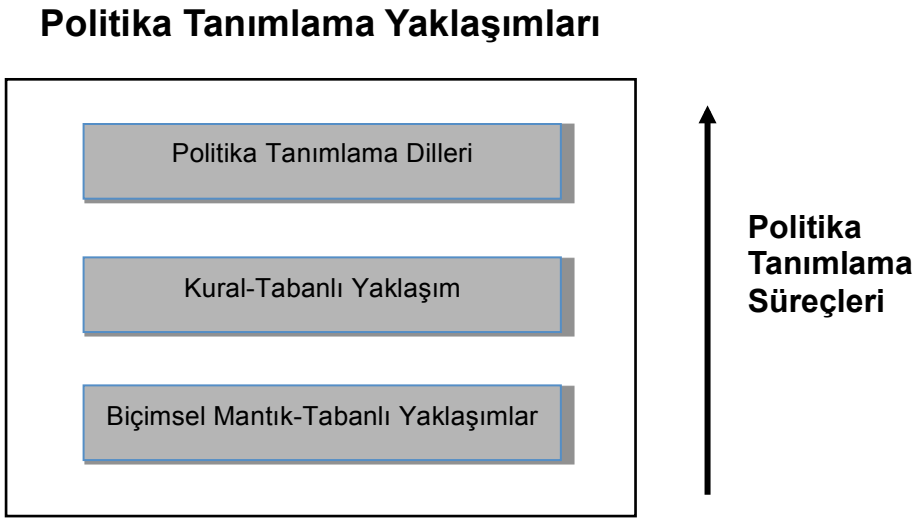
6. Mevcut ortamlara uygulanabilirliği: Bir bağlam modelinin dağıtık bilgisayar ortamı üzerindeki mevcut alt yapıya uygulanabilir olması çok önemlidir.

2.2 Politikalara Genel Bakış

Bu bölümde bilişim bilgi kaynaklarına erişim kurallarını belirleyen politikaların tanımı ve sınıflandırılması, ayrıca politikalar için kullanılan terminolojik kavramlar ele alınarak, erişim kontrol politika modelleri ile ilgili araştırmalar hakkında söz edilecektir.

2.2.1 Politika ve Terminolojisi

Politika üzerinde çalışma yapan araştırmacılar tarafından farklı tanımlar verilmiştir. Damianou ve Bandara [5] tarafından yapılan tanımda politika – sistem davranışlarını yöneten kurallar kümesi olarak ifade edilmektedir. Sözlüklerde ise politika, bir eylem planı olarak tanımlanmaktadır. Bu bağlam politika, sistem davranışlarında rasyonel sonuçların ulaşılması amacıyla kararları yöneten bir ilke veya kuraldır [2].



Şekil 2.2 Politika Tanımlama Yaklaşımları [68]

Aynı zamanda IETF (Internet Engineering Task Force) tarafından yapılan tanımlamaya göre, politika - o anki ve ilerdeki eylem süreçlerinin yönlendirilmesi ve belirlenmesi için bir amaç veya yöntem olarak ifade edilmiştir. Yaygın kullanılan diğer tanımlardan birisi de, sistemin koşullarını

belirleyen bir varlık tarafından tekrarlanan ve önceden belirlenmiş eylem planları, politika olarak adlandırılmaktadır.

Bir politika tanımlama süreci: Politika uygulanacağı uygulama çeşitleri ve mevcut politika araçlarının oldukça fazla olması gibi iki nedenden dolayı kolay bir işlem değildir. Finansal, ticari, askeri, bilişim güvenliği, sosyal gibi birçok çeşitli politika alanları mevcuttur. Böyle bir politikanın kategorize edilmesi kullanım alanına göre belirlenmektedir. Örneğin, askeri alanda politika belirlenmesinin ana konsepti gizliliğe dayanırken, ticari politikada ise ana konsept çoğunlukla bütünlüğü ile ilgilidir.

Politika ifade etmenin üç yolu vardır(Şekil 2.2): politika tanımlama dilleri, kural-tabanlı tanımlama ve biçimsel mantık diller. Bir güvenlik yöneticisi açısından bakıldığında, etki alanı yönetimi için bir politika tanımlama (üst düzey) dili kullanımı söz konusudur. Kural-tabanlı yaklaşımı, “if (koşul) then (eylem)” şeklinde politika ifade edilmesidir. Son olarak da, mantık-tabanlı yaklaşımı, politika özelliklerini analiz edilmesi için gereklidir.

Politikaları kategorize etmenin birden çok perspektif yönleri vardır. Genellikle bir sistem üzerindeki işlevselliği veya niteliğine göre politika sınıflandırılması yapılmaktadır. Chadha ve Kant [3] tarafından yapılan çalışmalarda da ifade edildiği gibi “Sistem davranışlarını dikte eden kural”, “Erişim izni ya da reddetme kurallar” ve “Kısıtlar veya parametreler” olarak politika kategorizasyonu yapılmaktadır.

Politika - Sistem Davranışlarını Dikte Eden Kural

Bu politika sınıflandırması en yaygın kullanılan türdür. Yordamsal nitelikteki bu tür kurallar spesifik koşullar altında özel eylemlerin gerçekleştirilmesini belirtir. Ya da bu tür kurallar, sistemin davranış şeklini dikte eder. Örneğin: “Her gün saat 00.00’da veri tabanı yedeklemesi yapılır.” , “Her gün saat 21.00’da sistem kapatılsın”. Her ikisindeki kurallarda belirli bir spesifik koşul veya durumda hangi eylemin tetikleneceği belirtilmektedir.

Politika – Erişim İzni ya da Reddetme Kural

Bu türdeki politikalar da kurallar biçiminde olup, yordamsal olmaktan ziyade daha çok deklaratif şekildedir. Bunlar genelde belirli bir eylem gerçekleştirmek için varlıklara erişim izninin ya da reddinin tanımlanması için kullanılır.

Politika - Kısıtlar veya Parametreler

Politikalar, bir sistem kuralı olarak kısıt veya parametreleri tanımlamak için kullanılmaktadır. Bu kısıtlar, bildirge şeklinde belirtilir ve sistem üzerinde her zaman pozitif olan spesifik ilişkileri ile ilgili ifadelerin beyanını sağlar. Bu kısıtlar sistem kurallarını belirlediği için politika olarak adlandırılmaktadır. Bu tür politikalar üst düzeyli nesne ve kaynaklara ulaşılmasını sağlamak için kullanılır. Örneğin, bu kısıtların askeri alanda kullanımında, çeşitli kaynaklara erişimi üzerinde direktif olarak gelir: kurumsal direktifler, işlevsel yönetmenlik, yönetimsel kılavuzlar. Bu biçimdeki politikalar sistem yönetimi tarafından doğrudan anlaşılabilir olmayabilir. Bunların anlaşılabilir olması için sistemde kullanılabilir yapılara dönüştürülmesi söz konusudur.

2.2.2 Güvenlik ve Erişim Kontrol Politikaları

Güvenlik politikaları, kimliği doğrulanan öznenin (kullanıcı) nesne üzerinde spesifik eyleminin gerçekleştirilmesi yetkisini tanımlamaktadır [6]. Güvenlik politikası, sistemin gizliliği ve güvenliğinin sağlanması amacıyla bilgilerin paylaşımı ve erişimin yönetildiğine ait kurallar ve önlemlerdir.

Erişim Kontrolü politikaları, sistem üzerinde daha fazla güvenliği temin eden erişim denetimini sağlayan güvenlik politika türüdür. Erişim kontrolü politikalarının bir kaç türü mevcut olup, şöyle sıralanabilir:

- Yetkilendirme politikası (Authorization policy): bir öznenin nesneler kümesi üzerinde gerçekleştirdiği etkinlikleri tanımlar. Böyle bir politika türü, erişim kontrolü politikalarının özünü temsil eder. Pozitif yetkilendirme politikası, bir öznenin nesne üzerinde eylem gerçekleştirme izni tanımlar. Negatif yetkilendirme politikası ise bir öznenin nesne üzerinde eylem gerçekleştirme reddini ifade eder.
- Yetki aktarma politikası (Delegation Policy): bir öznenin sahip olduğu yetki kümesini diğer özneye aktarma işlevleri için kullanılmaktadır. Yetki aktarılan özneler yetki alanları (grantees), yetki aktaran öznelere ise yetki veren(grantors) olarak adlandırılmaktadır.
- Zorlayıcı politika (Obligation policy): çok özel nesneler üzerinde özne tarafından yapılması zorunlu eylemler kümesi durumunu tanımlar. Yetkilendirme politikalarının aksine, zorlayıcı politikaları özne tabanlıdır

(yani özne politikayı yorumlar ve hedef nesne üzerinde eylemler gerçekleştirir). Zorlayıcı politikaları genelde olaylar tarafından tetiklenir.

- Kısıtlama politikası (Refrain policy): Bir öznenin nesne üzerinde gerçekleştirilmemesi (sakıncalı) gereken eylemleri tanımlar. Bir anlamda negatif yetkilendirme politikalarına benzer işlevi görür. Fakat kısıtlama politikası özne tabanlıdır.

2.2.3 Yönetim Politikaları

Yönetim politikaları, yönetim sistemin değişime uğratmaksızın yönetim yaklaşımının basitçe değişmesine olanak sağlayan dinamik uyarlanabilir yönetim stratejilerinin tanımlanmasında kullanılmaktadır. Birçok politika tabanlı yönetim yaklaşımları, basit bir koşul ve eylem içerikli olarak kolayca değişen koşul-eylem kuralları kullanmaktadır [4]. Bu alandaki çalışmaların en önemli kısmı IETF tarafından önerilen politika modelini temel alarak, **if <koşul (x) > then <eylem(x)>** şeklinde kural tanımıyla işlem gerçekleştirmektedir. Burada kuralın koşul kısmı VEYA ya da VE işlem ifadeleriyle tanımlanmaktadır. Bu kuralın eylem kısmı ise belirtilen koşulun yerine getirilmesi durumunda gerçekleştirilen eylemler kümesi olabilir. Bu tür politika kuralları, zorunlu politika davranışlarına benzer işlemi sergiler.

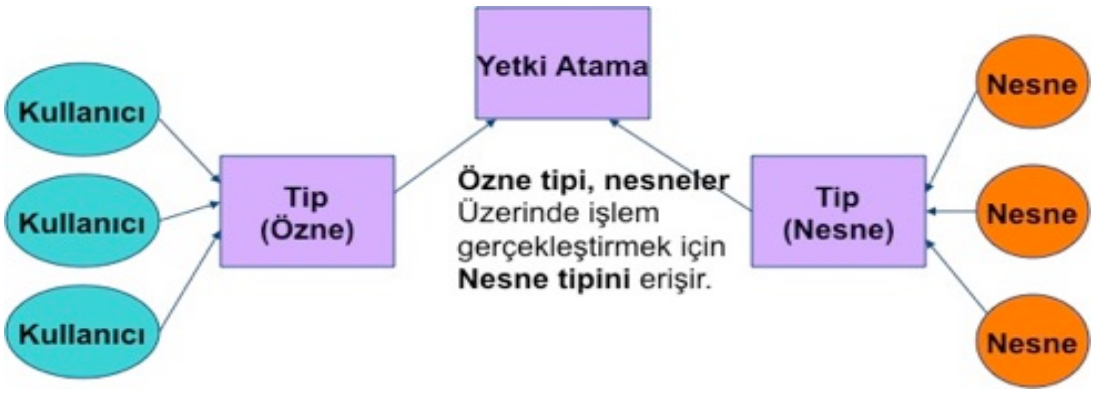
Bazı politika tabanlı yönetim sistemlerinde, karmaşık politika kümeleri uygulanmaktadır ve bu tür sistemlerin dinamik yapısından dolayı, politika değişmesi ve tutarsız politika çakışmalarına neden olabilir. Politikaların çakışması derken, tutarsız koşullardan kaynaklanan bazı politikaların uygulanması sonucunda diğer politikaların uygulanmasını geçersiz kılması anlaşılır. Politika kuralları içerisinde ortaya çıkan bu sorunun çözüm yollarından biri de, öncelikli değerlerle ilişkilendirilerek tutarsız kuralları ortadan kaldırmaktır. Ancak bu yöntem, karmaşık politika kurallarına sahip olan büyük ölçekli sistemlerde yetersiz kalmaktadır.

2.3 Geleneksel Erişim Kontrolü Modellerine ilişkin Çalışmalar

Bilişim teknolojisi ve bilgi güvenliği konusunda yapılan çeşitli çalışmalar ve bu yönde gösterilen çabalar, bilgi kaynağının kullanılması ve güvenli erişim düzenekleriyle korunması üzerine odaklanmıştır. Erişim kriterleri roller, grup, konum, zaman, işlem türleri olarak düşünülebilir:

- Roller – Belirli işlemleri gerçekleştiren kullanıcıya bu tür hakları atamanın en etkili bir yoludur. Bu rol görev atama veya işleve dayalı olabilir.
- Gruplar – Erişim kontrol hakların atamanın en etkili yollarından biridir. Birçok kullanıcının aynı tip bilgi ve kaynaklara erişimi gerekiyorsa, öncelikle onlar bir gruba dahil edilir ve daha sonra bu gruba gerekli hak ve yetkiler atanır. Böylece yönetim kolaylığı sağlanır.
- Konum (fiziksel veya mantıksal) – Kaynak bilgilerine kısıtlı erişimi için kullanılabilir. Yetkisiz kişilerin bulunduğu ortamına göre kısıtlı erişim politikaları uygulanabilir.
- Zaman (Geçici sınırlama) - Belirli eylem veya hizmetlerin erişimlerini zamansal olarak sınırlanabilir.
- İşlem türleri – Bilgiye erişim sürecindeki belirli işlev tipleri ve bilgi üzerinde gerçekleştirilen işlemlerin kontrolü için kullanılır.

Bu çerçevede geleneksel erişim kontrolü modelleri (Şekil 2.3) üçe ayrılabilir: Zorunlu Erişim Kontrolü (MAC), İsteğe Bağlı Erişim Kontrolü (DAC) ve Rol Tabanı Erişim Kontrolü (RBAC) [14].

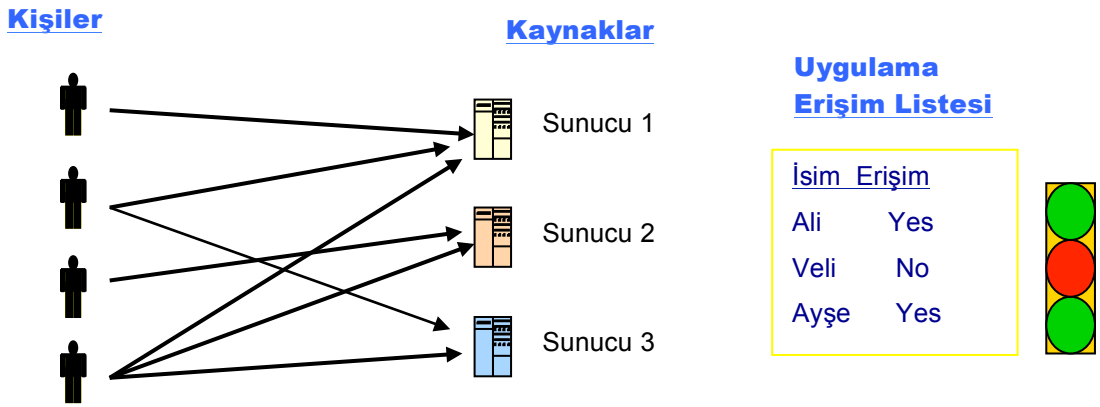


Şekil 2.3 Gelekneksel Erişim Kontrolü Modeli [88]

Bu modeller kapalı sistemler üzerinde başarılı olmasına rağmen, modern bilişim teknolojileri ortamında bilgi ve sistem güvenliği için erişim kontrolü sorunu önemli bir sorun olmaya devam etmektedir. Bilgi kaynağına kimin erişim izni ve nesneler üzerinde hangi erişim yetkilerine sahip olduğunu belirleme yeteneğini kazandırma konseptleri erişim kontrolü modellerinin kilit ilgi odağıdır [17].

2.3.1 İsteğe Bağlı Erişim Kontrolü (DAC)

İsteğe bağlı erişim kontrolü - yetkili kullanıcıların belirlenmesine dayanarak, mevcut kaynak bilgisi ve hizmetlere kısıtlı erişimi sağlayan bir düzenek olarak ifade edilebilir [9]. DAC, kullanıcı odaklı olup, her bir sistem kaynağı bir ya da daha fazla varlığın sahipliğine atanmıştır. Günümüzün birçok işletim sistemleri yetki denetim düzeneği olarak DAC modelini kullanmaktadır. DAC modeli, nesne sahibi veya yaratmaya kimin yetkisi olduğunu, kullanıcının erişim haklarını belirleyen ve koruma kararları türetebilen esnek erişim kontrolü sağlamaktadır(Şekil 2.4).



Şekil 2.4 İsteğe Bağlı Erişim Kontrolü Modeli [11]

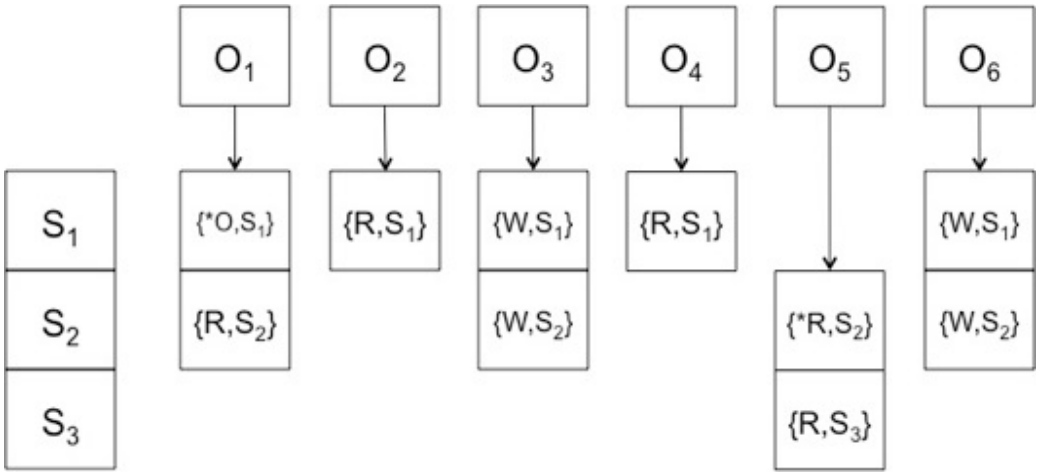
	x.doc	pacs.exe	hu.com
Ali	{}	{exec}	{exec,read}
Mehmet	{read,write}	{exec}	{exec,read,write}

Çizelge 2.1 Erişim Kontrol Matrisi

DAC modelinde kullanıcılar kendilerine verilen yetki sınırları dahilinde diğer kullanıcılara erişim yetkileri verebilir ya da kısıtlamalar getirebilir. Yani, sistem kullanıcılarının, diğer kullanıcılar tarafından kendi denetimleri altında olan nesnelere erişimine izin verip vermemesini sağlamaktadır. Erişim kontrolünde kullanılan kaynak ve sahibi kavramı en genel ve gerçek dünyaya uyan bir modeldir.

DAC modelinin esnekliği çok çeşitli sistemler ve uygulamalar için isteğe bağlı erişim denetimini uygun kılmaktadır. Genellikle bu tür erişim kontrolü, işletim sistemlerinin klasör ve dosya yetkilendirmelerinde yaygın olarak kullanılmaktadır. Böylece kullanıcıya ait klasöre ve dosyalara erişim için diğer kullanıcılara yetki veya kısıtlamalara getirebilir. Bu model yapı olarak erişim kontrol matrisi olarak ifade edebilir.

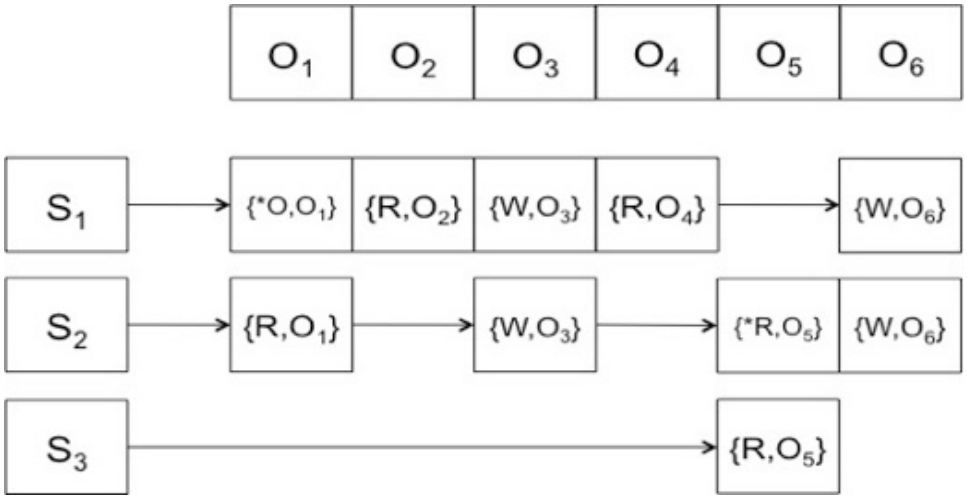
Erişim kontrol matrisi, sistemdeki öznelerin (kullanıcı, süreçler) nesnelerin üzerindeki kullanım haklarının tanımlandığı bir matristir(Çizelge 2.1). Bu matris yapısında, sütunlar erişim kontrol listesi (ACL) tablosu, satır olarak da yetenekler (capability) listesi (CL) tablosunu (Çizelge 2.2) ifade edilir. ACL listesinde ikililer halinde nesneye erişecek özneler ve öznelerin erişim bilgileri bulunur(Şekil 2.5):



Şekil 2.5 ACL Tablosu [11]

Örneğin:

acl(Dosya1)={ (süreç1, {read, write, own}), (süreç2, {append}) }



Şekil 2.6 CL Tablosu [11]

Bir özne ACL 'de yer almıyorsa ilgili nesne üzerinde herhangi bir erişim hakkında sahip olmadığı anlamına gelir. Bir çok öznenin aynı nesneye erişim haklarına sahipse grup tanımlayarak ACL listesinde (kullanıcı, grup, haklar) biçiminde erişim hakları tanımlanır.

Yetenekler listesi (CL) ise bir öznenin hangi nesnelere, hangi erişim hakları olduğunu tanımlar (Şekil 2.6).

Örneğin:

Ali	pacs.exe: {exec}	hu.com: {exec,read}

Çizelge 2.2 CL Listesi

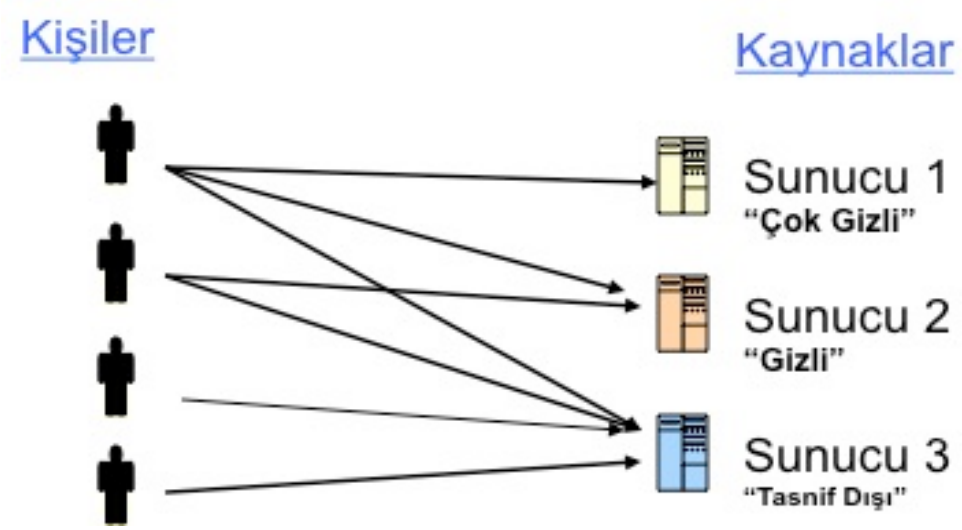
Sonuç olarak, kullanıcının nesne ile ilgili istekleri, belirtilmiş yetkiler kontrol edilerek gerçekleştirilmektedir (Sandhu ve Samarati, 1994). DAC, kullanıcıların sistem kaynaklarını denetleme kavramı üzerine yoğunlaşmaktadır. Gerçekleştirilmiş birçok politikanın bir şekilde ilişkilendirildiği isteğe bağlı erişim denetimi yaygın bir şekilde benimsenmektedir.

Ancak, bilginin akışını ilgilendiren herhangi bir biçimsel güven sağlanmaması DAC modelinin olumsuz yönlerinden biridir. DAC politikalarında erişim yetkilerinin dağıtılması denetimsizdir ve erişim yetkilendirme sürecinin

kullanıcılara bırakılması güvenlik açıkları oluşmasına neden olabilecek erişim kontrolü politikalarının uygun biçiminde uygulanamayabilir. Bu çerçevede, dağıtık bir yapıda gerçekleşen erişim yetkilendirme sürecinde kullanıcılara verilen yetkilerin denetlemesini zorlaştırarak merkezi denetimi imkânsız kılmaktadır.

2.3.2 Zorunlu Erişim Kontrolü (MAC)

Zorunlu erişim kontrolünde bir kaynağın erişim yetkileri, DAC modelinden farklı olarak bilgi kaynağının sahibi tarafından değil sistem tarafından belirlenmektedir(Şekil 2.7). Zorunlu erişim kontrolü – kullanıcıların, kaynak içeriğini belirleyen "erişim duyarlığına" dayalı nesnelere kullanıcının kısıtlı erişim işlemini gerçekleştiren bir süreçtir. Bu modelde, kaynak ve sahibi kavramı kullanılmamaktadır(Benantar,2006).



Şekil 2.7 Zorunlu Erişim Kontrolü Modeli [11]

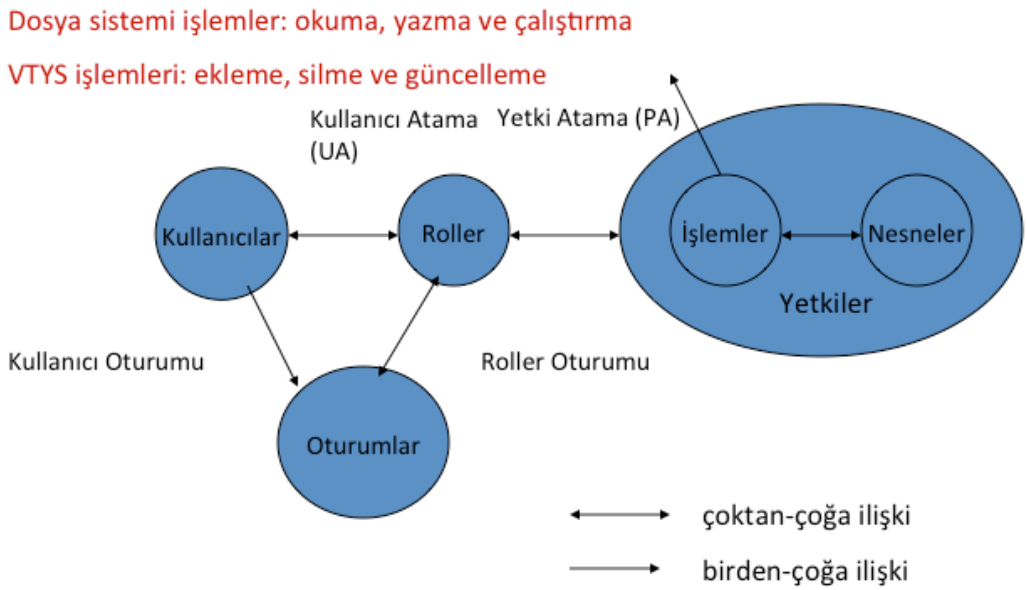
MAC modelinde, sistem varlıklarının kaynağa erişimin dağıtımına yönelik hiçbir denetimi yoktur. Bunun yerine, erişim özellikleri güvenilir bir yönetici tarafından bilgi kaynağına hangi kullanıcının nasıl bir şekilde erişeceğini belirten kurallar üzerinde yetkilendirmektedir. Yani, merkezi yönetim tarafından önceden belirlenmiş politika kurallarına göre kaynaklara erişim denetimi yapılmaktadır. Genelde, gizlilik düzeyi çok yüksek olan askeri kurumlarda MAC erişim kontrol modeli yaygın kullanılmaktadır. Bu bağlamda, kaynak bilgileri "Tasnif Dışı", "Resmi", "Kısıtlı", "Gizli" ve "Çok Gizli" olarak kategorizasyona göre etiketlendirilerek, kullanıcıların hangi bilgi kategorisine erişebileceği ile ilgili yetki düzeyleri tanımlanmaktadır.

MAC modelinde, kullanıcının belirli bir gizlilik düzeyindeki bilgiye ulaşması için en az o düzeydeki erişim yetkisine sahip olmalıdır. Aynı zamanda “Bilmesi Gereken” ilkesi temelinde erişmek istenilen bilgi üzerinde işlem yapabilmesi için ihtiyacı olması gerekir. Böylece kullanıcının yeterli düzeyde yetkisi olmasına rağmen, bilgiye ihtiyacı yoksa erişimi engellenir.

MAC modeli, erişim kontrolü politikalarının zorunlu olarak uygulanmasını gerektirir. Bu yöntemle, önemli bilgi kaynaklarının barındırıldığı ortamlarda yüksek güvenliği sağlamak amacıyla çok sıkı denetim yapabilmeye olanak tanır. Bu model, DAC modeline göre daha sağlam ve güvenli erişim düzeneği olup, “dolaylı bilgi akışını” kontrol eder.

2.3.3 Rol Tabanlı Erişim Kontrolü (RBAC)

Şu ana kadar yapılan araştırma ve çalışmalar sonucunda farklı yaklaşımlar temelinde belirli üstünlüklere sahip çeşitli erişim kontrolü modelleri önerilerek hayata geçirilmiştir.

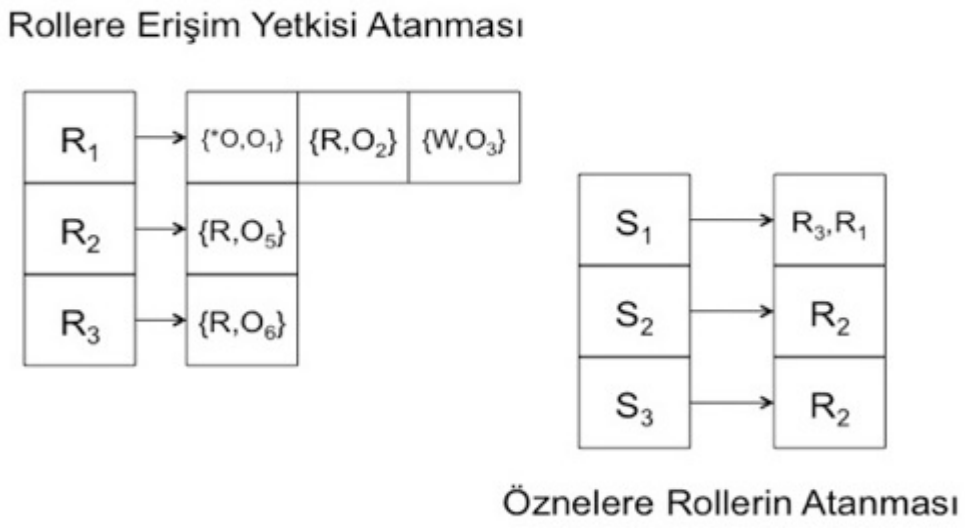


Şekil 2.8 Rol Tabanlı Erişim Kontrolü Modeli [87]

Bu çerçevede, güvenli erişim kontrol işlemlerinin en önemlisi, rol-tabanlı erişim kontrol modeli olmuştur. RBAC modeli, mevcut diğer erişim kontrolü modelleri üzerinde daha da avantajlı olduğundan büyük ilgi görmüştür. Genel olarak rol tabanlı yetkilendirme modeli “**Kullanıcı -> Roller -> (Kaynak, İşlem)**” şeklinde tanımlanabilir. Bu yapıda, kullanıcılar bir veya birden fazla role dahil edilerek, yetkiler de bu rollere atanmaktadır(Şekil 2.8).

Böylece, rollerin değişmeyeceği veya daha az değişeceği öngörülerek, kullanıcı değişimine bakılmaksızın yetkilendirme yapısının değişmemesi sağlanmaktadır. Bu kapsamda, RBAC modeli kurallarının kategorize edilirken üç ana konseptten söz edilebilir(Şekil 2.9-Şekil 2.10):

- Rol Atama – Özne, kendisine atanan bir role sahip olduğu sürecin ilgili nesneler üzerinde işlem yapabilir.
- Rol Yetkisi – Özne, sadece sahip olduğu rolün yetkisi dahilinde işlem yapabilir.
- Yetkilendirme İşlemi – Öznenin rolü için ilgili nesneye yetkilendirme sürecinden sonra özne ilgili nesne üzerinde işlem yapabilir.



Şekil 2.9 RBAC İşlem Tablosu [11]

RBAC üzerinde yapılan araştırma çalışmalar sonucunda dört ayrı RBAC modelinin olduğu söylenebilir:

- RBAC0(Düz RBAC) – kullanıcıya doğrudan rol ataması gerçekleştirilerek, her bir kullanıcıya eş zamanlı olarak roller aktif edilir. Ancak burada hiyerarşik yapı desteklenmemektedir. Bu model biçimsel olarak söyle ifade edilebilir:
    - U,R,P,S sırasıyla (kullanıcılar, roller, yetki izinler ve oturumlar);
    - Statik ilişkiler: PA $\subseteq$ P × R (rollere yetki atama), UA $\subseteq$ U × R (kullanıcıya rol atama);
    - Dinamik ilişkiler: kullanıcı - S $\rightarrow$ U (her oturuma bir kullanıcı), roller - S $\rightarrow 2^R$,

$R(s) \subseteq \{ r \mid (U(s), r) \in UA \}$, $PA(s) = \bigcup_{r \in R(s)} \{ p \mid (p, r) \in PA \}$;

- RBAC1(Sıradüzensel RBAC) - roller hiyerarşik yapıda olup, erişim yetkilerinin kalıtımsal ve devir etme özelliklerini destekler. Bu modelin biçimsel ifadesi:
  - $RH \subseteq R \times R$ (r1 ≥ r2 – r1 rolü r2 rolüne göre daha kıdemli);
  - Roller: $S \rightarrow 2^R$, $R(s) \subseteq \{ r \mid \exists r' [(r' \geq r) \& (user(s), r') \in UA] \}$,

    $PA(s) = \bigcup_{r \in R(s)} \{p \mid \exists r'' [(r \geq r'') \& (p, r'') \in PA] \}$;

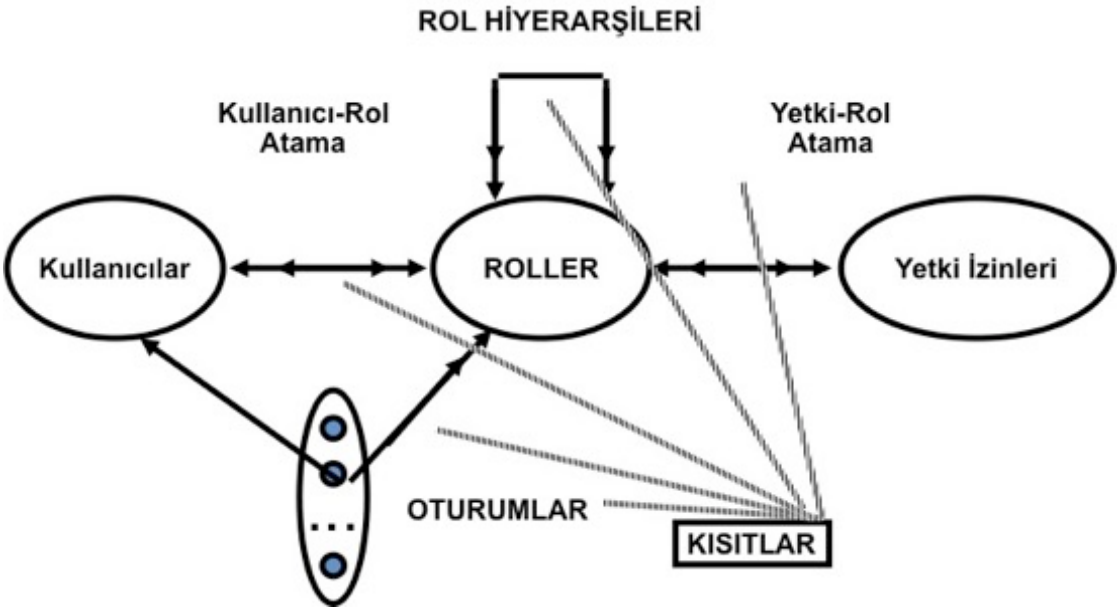
- RBAC2 (Kısıtlı RBAC) – rol bağlantılarındaki koşul kısıtlamalar söz konusudur. Yani bazı rollerin atanabilmesi için bazı koşullar yerine getirilmelidir ve roller hiyerarşik yapıda değildir.

RBAC3 (Simetrik RBAC) - rol bağlantılarındaki koşul kısıtlamaları ve roller hiyerarşik yapıyı destekler ve NIST tarafından önerilen standart modelidir(Şekil 2.11).

Şekil 2.10 RBAC Yetkilendirme Süreci [88]

Standartlar ve Teknoloji Ulusal Enstitüsü (NIST – National Institute of Standards and Technology) tarafından tanımlanan rol-tabanlı erişim kontrolü modeli, diğer RBAC modelleri için standart servis olarak geliştirilmiştir. Erişim kontrolünün ana konularından biri de, kullanıcılar ve kaynakların dağıtık olduğu bir dağıtık ortamda, büyük ölçüde özne ve nesnelerin yönetilmesine ihtiyaç duyulur. Grup, rol, seviye ve benzer yaklaşımlarla söz konusu problemlerin çözümü hedeflenmiştir. Örneğin, bir özne aynı yetkilere sahip olan bir grup çerçevesinde değerlendirilmiştir. Buna benzer olarak nesne de,

güvenlik yaklaşımına göre farklı seviyelerde (çok gizli, gizli, güvenilir v.s.) sınıflandırılabilmektedir. Ayrıca erişim yetkileri ayrıcalık kümeleri altında toplanarak, basit bir erişim kontrolü yönetimi sağlanabilir. Güvenlik politikalarının basitçe yönetimi ve aynı zamanda erişim kontrolü modellerinde ifade gücünün geliştirilmesi, ideal erişim kontrolü modelinde beklenen esnekliği kazandırır ve politikaların özelleştirilebilir olmasını sağlar.



Şekil 2.11 RBAC3 NIST Modeli [87]

Büyük ölçekteki kullanıcılar, nesneler, roller ve program bileşenlerine sahip gelişmekte olan dağıtık sistemleri, mevcut geleneksel erişim kontrolü modellerinin (MAC ve DAC) etkinliğine büyük ölçüde meydan okumaya başlamıştır.

Genelde erişim kontrol modellerinde rol konsepti özneye göre daha geniş olup, herhangi bir kurumun mantıksal yapı tanımlamasında, ayrıca veri tabanı yönetim sistemleri, güvenli yönetimi ve iş alanlarında geniş çaplı kullanılabilir. RBAC modelinin en önemli avantajlarından biri de, roller ile ilişkili işlemlerin zaman içinde çok az değişime uğramasıdır. İnsanlar genellikle kendi işini değiştirse bile, ama işler kendince değişemez. Ayrıca çoğu insan aynı rol ve yetkiye sahip olabilir. RBAC politikaları kişiye özgü değil iş rolüne göre yazılır. Kişinin fiilen değişmesi, RBAC politikasını etkilemez. Bu özellik, özellikle büyük kurumlarda güvenlik yönetimini oldukça kolaylaştırır.

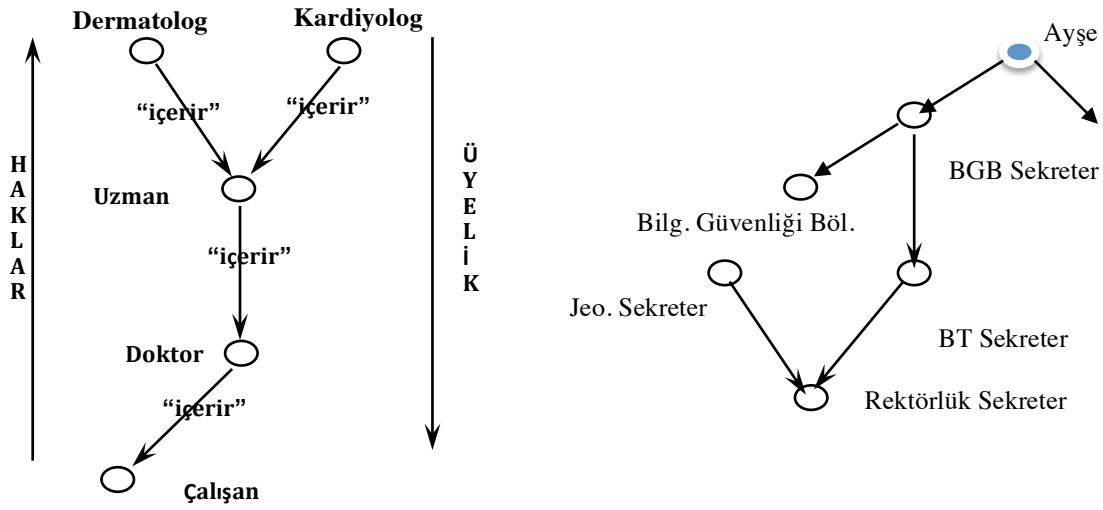
RBAC modelinde kullanıcı, izinlerini sistemde tanımlı olan rollerine göre elde etmektedir. Böylece, kullanıcı rolleri ile ilişkili olan bütün izinlerini kalıt almaktadır ve bu rol sıradüzeni ayrıca politikaların tanımlanmasını da basitleştirmektedir (Abou El Kalam v.d., 2003; Cuppens ve Miège, 2003).

RBAC modellerindeki roller hiyerarşik yapıda olup(Şekil 2.12), erişim yetkilerinin kalıtımsal ve devir etme özelliklerini destekler. Erişim yetkileri - kıdemli rolden aşağıya doğru kalıtsal olarak geçer ve aynı anlamda erişim yetkisi bir rolden diğer role devir edebilir. Yetki devri, etki alanları arasında gerçekleşir. Birçok kullanıcı aynı role sahip olduğu sürece RBAC modelinde yönetilecek kimlik ve atama sayısı azalır.

Ayrıca rollerin belirlenmesinde “yukarıdan aşağıya”, “aşağıdan yukarıya” veya her ikisinin de kullanıldığı “hibrit” yaklaşımlar kullanılmaktadır:

- Yukarıdan aşağıya yaklaşımda, rollerin kurum içindeki görev ve sorumluluklara göre hiyerarşik sıralanması söz konusudur. Ancak bu yaklaşımda rollerin oluşturulması uzun zaman almaktadır;
- Aşağıdan yukarıya yaklaşımda, sistem üzerindeki kullanıcıların mevcut yetkilere göre hiyerarşik sıralanması söz konusudur. Bu yaklaşımda sistem üzerindeki çok sayıda kullanıcı yetkisinin incelenmesi ve analiz edilmesi gerekir. Ancak sistem üzerinde “olması gereken yetkiler” yerine “mevcut” yetkilerin kullanımı tutarsız hatalara neden olabilir. Bu ise görev ayrılığı ve “en az yetki” ilkelerine uygun değildir.
- Hibrit yaklaşımda ise her iki yaklaşım bir arada kullanılmaktadır. Bu yaklaşımda rollerin oluşturulması süreci daha hızlı olup, sistem üzerindeki yansımaları kolaylıkla ilişkilendirilebilir.

RBAC modelinde sistem yöneticisi tarafından hangi kullanıcının belirli bir kaynak nesnesine erişim yetkisi olduğu veya söz konusu kullanıcının ne tür izne sahip olduğu ve hangi kaynak nesneye erişebildiği kontrol edilebilir. RBAC modelinin başka ayırt edici özelliği, herhangi bir politika güdümlü olmaması ve güvenlik politikalarının gelişigüzel ifade edilebilmesidir. Bu anlamda RBAC, bir kurumun güvenlik politikasındaki değişiklikler güvenli sistem üzerinde yeniden modelleme yapmaksızın kolayca uyarlanabilmesidir.



a-Kısıtlı Hiyerarşiler b-Genel Hiyerarşiler

Şekil 2.12 Rol Hiyerarşileri

RBAC politika bağımsız olmasına rağmen, üç iyi bilinen güvenlik ilkesini doğrudan destekler: en az yetki ayrıcalığı, görevlerin ayrılması ve veri soyutlamasıdır. Fakat RBAC düzeneğinde - kullanıcı-rol ve rol-izin atama süreçlerinde yönetimsel işlemlerin zorunlu olması, ayrıca roller ve izinlerin sayısındaki üstel artışın söz konusu atama işlemlerini daha maliyetli olması gibi bazı sorunlar bulunmaktadır (Yuan ve Tong, 2005a [41]). Bu yaklaşım, çok yüksek kullanıcı sayısına sahip olan büyük ölçekli açık sistemlerde yetersiz kalmaktadır. Başka bir deyişle RBAC modeli, açık veya dağıtık ortamı için ihtiyaç duyulan gereksinimleri karşılabilecek yeteneğine sahip değil.

Sonuç itibariyle RBAC modeli ile ilgili temel kavramsal çerçeve şöyle özetlenebilir:

Nesne – sistem üzerindeki kaynak bilgisidir;

İşlem (transaction) – nesneler üzerinde işlemleri gerçekleştirir. RBAC modelindeki tüm işlemler, kullanıcılar üzerinde değil rollerle ilişkilidir;

Erişim –özne ve nesne arasındaki özel etkileşim tipi;

Erişim Kontrolü – bir sistemin bilgi kaynaklarına erişimini sınırlayan süreç;

Yönetici Rolü – kullanıcılar kümesini, roller veya yetki izinleri güncelleme ya da kullanıcı veya yetki izni atama ilişkileri değiştirme yetkisine

sahip olan roldür;

Kısıt sınırlama – roller arasında ya da içindeki bir ilişki;

Grup – kullanıcılar kümesi;

Nesne – bilgi içeren veya kabul eden pasif bir varlık;

İzin – özne ile nesne arasındaki yetki etkileşim tanım tipi;

Rol hiyerarşisinde yetki izni devralma – işlem parçası olarak hiyerarşi içindeki rolün kullanılması için gereken koşulları tanımlar. Bu kapsamda 3 tip izin devralma mevcuttur: standart, sıkı ve hoşgörülü [Moy01].

Standart izni devralmada R rolünün kullanılabilmesi için, R kümesindeki bir rol için en az bir politika kuralı izin işlemi gerçekleştirmesi ve işbu rol üzerinde red işlemi ile ilgili herhangi bir politika kuralı bulunmaması gerekir.

Sıkı izni devralmada R rol kullanılabilmesi için, R kümesindeki her bir role izin işlemi veren sadece ve sadece en az bir politika kuralı mevcuttur ve söz konusu kümedeki herhangi bir rol için red işlemi ile ilgili politika kuralı bulunmaması gerekir.

Hoşgörülü izni devralmada, sıkı izni devralmayanın zıttı: R rol kullanılabilmesi için, R kümesindeki bir role izin işlemi ile ilgili bir politika kuralı mevcut ve aynı role red işlemi uygulayacak herhangi bir politika kuralı bulunmuyor.

Kaynak – bir işlevi yerine getirirken kullanılan bir nesnedir.

Rol hiyerarşisi – roller içinde kurulan ilişkiler;

Oturum - kullanıcıya ile roller kümesi arasındaki eşleştirme;

Özne – bir aktif varlık(personel, süreç veya aygıt);

Sistem yöneticisi – sistem güvenlik politikalarını belirleyen, yönetimsel rolü yerine getiren ve yetki izin işlemlerini izleyen birey;

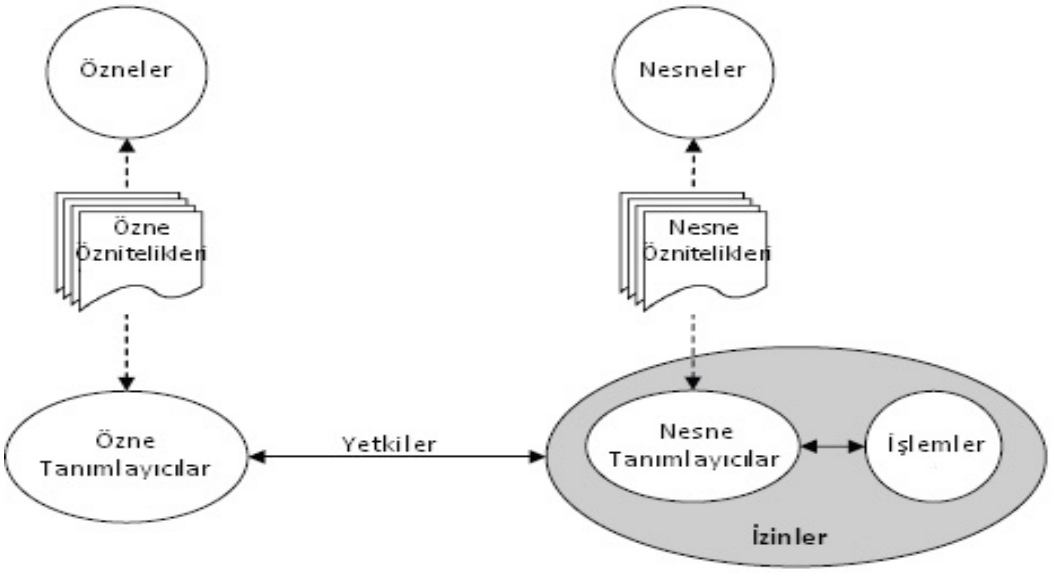
Kullanıcı – bir bilgisayar sistemiyle doğrudan karşılıklı etkileşimde bulunan kişi;

En az yetki – Kullanıcıya atanan Role ait sadece bir yetki izni verilir.

Görevler ayrılığı – Aynı kullanıcı farklı rollere sahip olabilir ve aynı kullanıcıya erişim denetim zayıflıklarına neden olacak yetkilerin söz konusu olduğu farklı rollere verilebilir. Yetkilendirme sürecinde söz konusu rollerin aynı kullanıcıya verilmesini engelleyecek, hassas görev tanımlama işlemi gerekir.

2.3.4 Öznitelik Tabanlı Erişim Kontrolü (ABAC)

Öznitelik Tabanlı Erişim Kontrolü, özne ve nesneler arasındaki erişim yetki izinleri tanımlama sürecini onların öznitelikleri üzerinde gerçekleştirmektedir(Şekil 2.13).



Şekil 2.13 ABAC Modeli [86]

Bu çerçevede, ABAC (Attribute-Based Access Control) modelinde özniteliklerin üç şekilde gösterilmesi söz konusudur: Özne, Kaynak ve Çevre öznitelikleri [41-42]. Burada Özne öznitelikleri, öznenin kullanıcı, uygulama ve işlem gibi kimliği ve nitelikleri ile ilişkilendirilmektedir. Kaynak öznitelikleri, sistem işlevi veya bilgi kaynağıyla ilişkilendirilmektedir. Çevre öznitelikleri ise durumsal ortam veya çevreyi ya da bilgi erişiminin gerçekleştiği bağlamı ifade etmektedir. Bu modelin biçimsel özellikleri aşağıda tanımlanmaktadır:

- S, R, E – Özne, kaynak ve çevre ortamı;
- SA_k ($1 \le k \le K$), RA_m ($1 \le m \le M$), EA_n ($1 \le n \le N$) - özne, nesne ve çevre varlıkları için öznitelikleri tanımlar;

- *ATTR(s)*, *ATTR(r)*, ve *ATTR(e)* – s özne, r kaynak ve e çevre için öznitelikleri belirleme ilişkileri:

  $ATTR(s) \subseteq SA_1 \times SA_2 \times ... \times SA_K$

  $ATTR(r) \subseteq RA_1 \times RA_2 \times ... \times RA_M$

  $ATTR(e) \subseteq EA_1 \times EA_2 \times ... \times EA_N$

- Bireysel niteliklerin değerleri ataması işlemi için fonksiyon kullanılır. Örneğin:
  Role(s) = "Servis Kullanıcısı"
  ServiceOwner(r) = "XYZ, Inc."
  CurrentDate(e) = "01-23-2005"

- **s** öznenin belirli **e** ortamda **r** kaynağa erişim ile ilgili kararı veren politika kural:

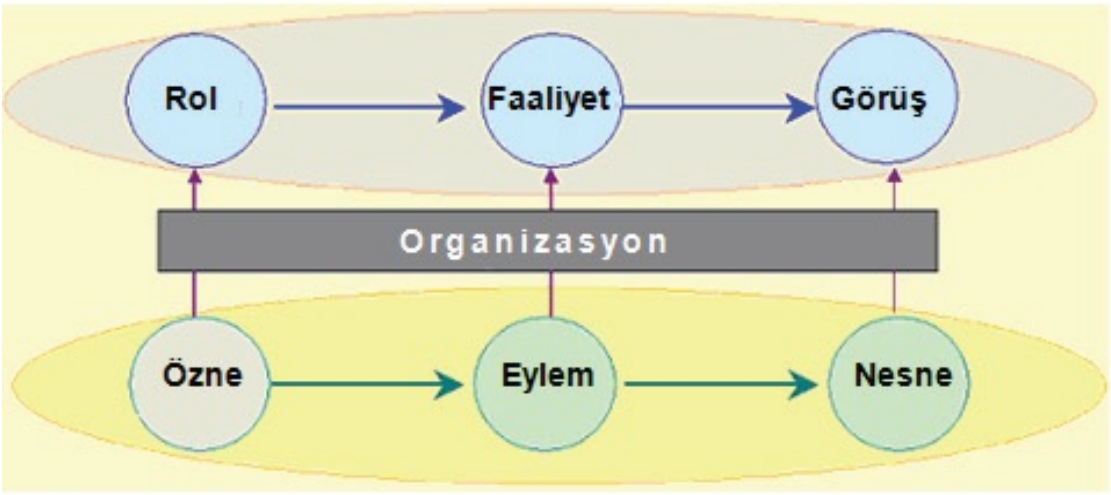
  $Rule\ X : can\_access(s, r, e) \leftarrow$
  $f(ATTR(s), ATTR(r), ATTR(e))$

ABAC modelinin eksik yönlerinden biri, politikaların tanımlanması ve yönetilmesi büyük ölçüde karmaşık yapısına sahiptir. ABAC genelde web ve veri tabanı uygulamaları gibi uygulamaların erişim denetimi katmanında kullanılmaktadır. Bu çerçevede, farklı uygulamalarının herbiri kendine özgü erişim denetim politikalara sahip olması, politika kurallarında önemli ölçüde çakışmalara sebep olmaktadır.

2.3.5 Kurum Tabanlı Erişim Kontrolü (OrBAC)

DAC, MAC ve RBAC gibi geleneksel erişim kontrolü modelleri kurumlara göre politika uygulamasında yaşanan sorunlar nedeniyle Kurum Tabanlı Erişim Kontrolü modeli geliştirilmiştir. OrBAC (Organization Based Access Control) modeli, somut (özne, eylem, nesne) ve soyut (rol, etkinlikler, görüş) olmak üzeri iki düzeyde oluşmaktadır(Şekil 2.14).

Burada rol, kuralların uygulandığı özneler kümesini, etkinlik - kuralların uygulandığı eylemler kümesini ve görüş ise kuralların uygulandığı nesneler kümesini temsil eder. En önemlisi OrBAC modeli dinamik bir politika yapısına sahip olup, izin, yasak, zorunluluk ve tavsiye politika nesnelerini içermektedir. Ayrıca OrBAC modelinde güvenlik politikalarının kolaylıklar oluşturulması için MotOrBAC [45] ara yüzü geliştirilmiştir.



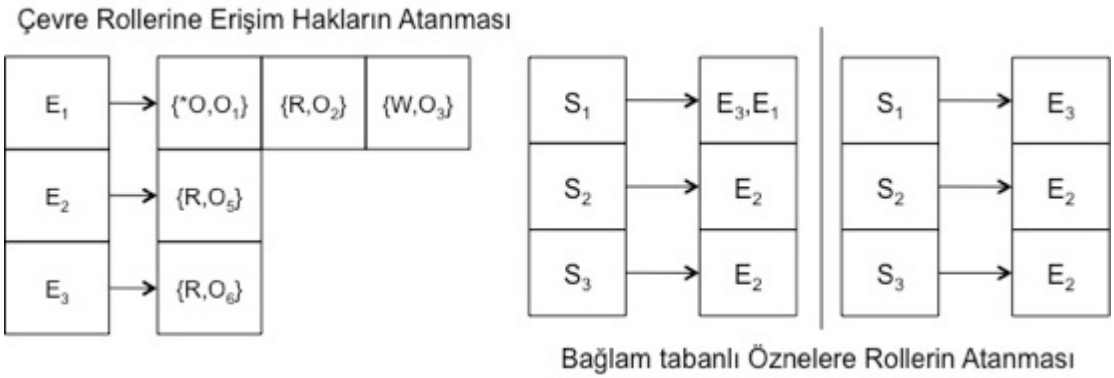
Şekil 2.14 OrBAC Modeli [86]

2.4 Bağlama-Dayalı Erişim Kontrolü Modellerine ilişkin Çalışmalar

Bu bölümde, kimlik ile bağlam bilgilerinin birleştirilmesi ya da eşleştirilmesi yoluyla erişim denetimi üzerinde herhangi bir karar verme işlemini gerçekleştiren bağlama-dayalı erişim kontrolü modellerine ilişkin ek çalışmalar ele alınmaktadır. Başka bir deyişle, bağlama-dayalı erişim kontrolü modeli – bağlam bilgileri içeren kısıtlar üzerinden kaynakları yöneten ve denetleyen ya da yeni oluşacak durumlara uyum sağlayan bir erişim denetimi düzeneğidir.

2.4.1 Rol-Tabanlı Erişim Kontrolü Modeli (RBAC) Türevleri

Burada, bağlam bilgileri üzerinde erişim karar düzeneğini kapsayan RBAC türevi olan bazı önemli modelleri incelenmektir. Bu modellerin arasındaki farklılıklar ve sınırlamaları gösterilerek, üstünlük ve eksikleri anlatılmaktadır. Kullanıcı ve izin atama işlevleri bağlamsal kısıtlarıyla denetleyen yeni bir tür bağlama-dayalı erişim denetim modeli Şekil 2.15'te sunulmuştur.



Şekil 2.15 Bağlama-Dayalı Erişim Kontrol Modeli

Bu modele göre, bağlamsal kısıt yerine getiren kullanıcıya ilgili rol atanarak, atanan rolü de bağlamsal kısıt işlevi üzerinden yerine getirecek yetki izni atanması gerçekleşmektedir.

2.4.1.1 Genelleştirilmiş Rol-Tabanlı Erişim Kontrolü Modeli (GRBAC)

Geleneksel RBAC modelinin genişletilerek daha güçlü bir hale gelmesini sağlayan Genelleştirilmiş Rol-Tabanlı Erişim Kontrolü (Generalized-Role-Based Access Control - GRBAC) modeli M.Moyer ve M.Ahmad tarafından bildirilmiştir. GRBAC ana görevi, yetkilendirme karar işlemi gerçekleştirme temeline dayanmaktadır ve politika tanımlarındaki herhangi bir tutarsızlık hatasını tespit edebilen politika üzerinde mantıklı denetimi destekler.

J.B.Filho ve H.Martin [28] tarafından önerilen GRBAC - bağlama-dayalı erişim denetimi alanında yapılan ilk modellerinden biridir. Bu model, özne, nesne ve çevre (*environment)* rolleri temelinde erişim kontrol karar süreci gerçekleştirmektedir ve genelde akıllı ev ortamı uygulamaları için önerilmiştir.

Söz konusu modelin ana görevi işlem üzerinde yetkiye karar verme temeline dayanmaktadır. Aynı zamanda, politika tanımlarındaki herhangi bir tutarsız hataları tespit edebilmek için politika üzerinde anlamlı kontrol düzeneğini desteklemektedir.

Özne/kimlik rolleri, geleneksel RBAC roller benzer şekilde olup, güvenlik politika tanımlanmasında kullanılabilen soyut bir özne özellikleri ilişkisidir.

Nesne rolleri, oluşturma tarihi, nesne tipi (görüntü, kaynak kodu, akıtmalı görüntü yayını-streaming video v.s.), duyarlık düzeyi (gizli, çok gizli, v.s.) veya

nesne içeriği ile ilgili bilgiyi içeren nesnenin sınıflandırılabilen özelliğine dayanmaktadır.

Çevre rolü, sistem bağlam olarak karar değerlendirme süreci anlamına gelen çevre bağlamını elde etmek için kullanılmaktadır.

Böylesi üçlü bir rol yapısı esnek ve güçlü ifade edebilme özelliğinin yanı sıra bu erişim kontrol modelini kullanılabilir kılmaktadır. GRBAC – roller ve işlemler kullanarak erişim kontrol karar değerlendirmesi gerçekleştiren işlem-tabanlı erişim kontrolü modelidir. Bu kapsamda GRBAC, hiyerarşi rol yapısını ve politika kuralları kullanarak, izin veya ret işlem kararı vermektedir.

Geleneksel RBAC modelinde, S özne O kaynak nesneye erişebilmesi için, S öznesine karşılık ancak bir R rolünün eşleştirme sürecinden sonra T yetkilendirme işlemi gerçekleşir(T->O kaynağa erişebilir).

Fakat GRBAC modelinde ise benzer yetkilendirme algoritmasına rağmen, biraz daha karmaşık bir yapıya sahiptir. Yukarıda söz edildiği gibi S - roller özne roller kümesine, O – nesne roller kümesine sahiptir. Ayrıca buna ek olarak da mevcut sistem çevre roller kümesi üzerinde karar işlemini gerçekleştirmektedir. Bu durumda, S öznenin O kaynak nesneye erişme yetkisi işlevini gerçekleştirebilmesi için,

1. $\exists R_s \in S$;

2. $\exists R_O \in O$;

3. Geçerli $\exists R_E \in E$;

4. Aktif bir RE çevre rolünün geçerli olduğu durumda R_S rolündeki öznenin R_O rolündeki kaynak nesnesine erişim yetkisini sağlayacak bir T işlemi gerçekleşir.

GRBAC'daki herhangi bir işlem(transaction) T=<S, O, E, op> olarak ifade edilerek, T işlemi için erişim kontrolü karar değerlendirme süreci aşağıdaki algoritma temelinde gerçekleştirilmektedir:

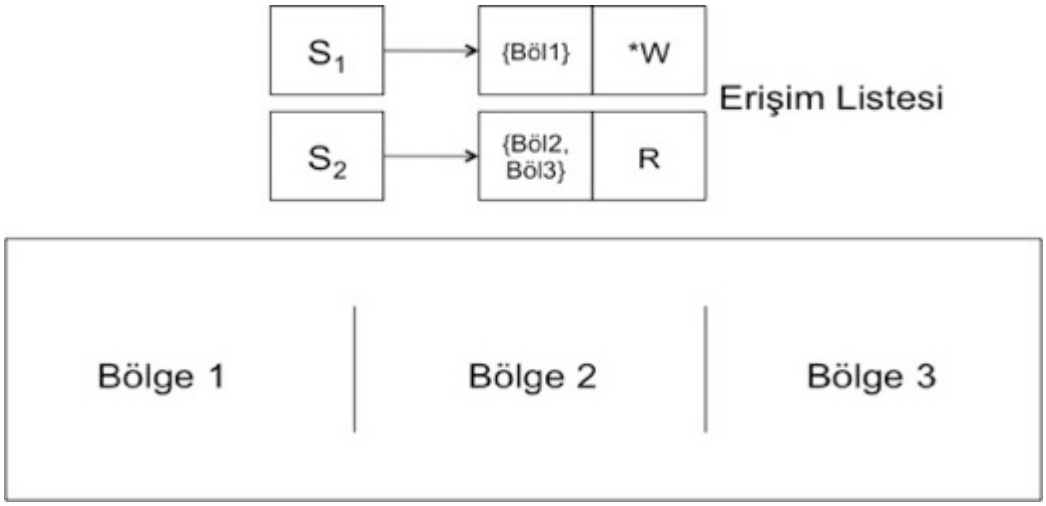
1. T=<S,O,E,op> işlemleri içeren tüm politika kurallarını değerlendirmeye alır. Burada S, O ve E sırasıyla S, O, ve E kümelerinin bileşenleridir;

2. Eşleştirme arasında pozitif izin bulunmuyorsa, reddetme isteği varsayılan olarak kabul edilir. T işlemlerinden en az birisi pozitif yetki ve diğer ise negatif yetki döndüğü durum için politika çatışması veya anlam tutarsızlığı meydana gelerek erişim isteği reddedilir. Aksi durumda, tüm eşleştirme işlemleri pozitif yetkiye sahip olduğunda erişim izin isteği döner.

Bu algoritma basit ve anlaşılabilir olmasına rağmen, rol hiyerarşi ve politika kural veri tabanı yapılarının optimizasyonu ve verimli indekslenme sorgularının uygulanabilirlik maliyetini yükseltmektedir.

2.4.1.2 Mekân-Zamansal Modeller

Dağıtık bilgisayar ortamında geliştirilen bazı erişim kontrolü modelleri genel olarak iki tip bağlam bilgisi kullanılmaktadır: zaman ve mekân [50,51]. Bu tip bağlam bilgileri kullanan bir RBAC modelinin türevlerinden biri de [48,50] tarafından önerilen TRBAC (Temporal Role-Based Access Control) modelidir. Bu model, zaman tabanlı erişim denetimi politikasını uyarlayan yeni bir düzenek üzerinden geçici kısıtlamalar getirmektedir. Buna göre kullanıcı için herhangi rol atama işlemi zamansal kısıtlamaya dayanılarak gerçekleştirilmektedir. GTRBAC (Generalized Temporal Role-Based Access Control) olarak bilinen diğer model ise aktif bir rol temelinde mevcut TRBAC modelinin genişletilmişidir. Burada rolü aktif hale getirmek kavramı rolü etkinleştirme kavramından farklı olarak, en az bir kullanıcı ile ilgili belirli bir oturumun etkin olması anlamını taşımaktadır ve kullanıcı tarafından geçerli bir rolün sahip olduğu tüm yetkileri alabilmektedir. Böylece rolün aktif kılmanın üstün tarafı, çalışan tüm süreç ve kullanılan kaynakları gözlemlemek açısından çalışan rolün belirlenmesinde yardımcı olmasıdır. GTRBAC modeli tarafından gerçekleştirilen “kullanıcı-rol” ve yetki atama süreçleri ile ilgili çoğu kısıt kuralları zamana göre etkinleştirme ve rol aktifleştirmeye dayanmaktadır[49].



Şekil 2.16 ST Modelleri [53]

H.Zhang [53] tarafından önerilen diğer SRBAC (Spatial Role-Based Access Control) modeli ise yer ve mekâna dayalı kısıtlama işlemi yaparak, kullanıcının bulunduğu yere göre erişim izni vermektedir(Şekil 2.16). Buna

göre yer ve mekân çeşitli alanlara ayrılarak, her biri farklı erişim yetki kümesine atanabilmektedir. Böylece kullanıcının erişim alabilmesi için sahip olduğu rolün bulunduğu konuma uygun koşulu yerine getirmelidir. Çizelge 2.3'te gösterildiği gibi her kullanıcının rolü bulunduğu özel mekan konumuna göre farklı yetkiye sahip olmaktır. Bu modelin ana sorunlarından biri de, uygun bir anlamsal yer ve mekân konum bilgisine sahip olmamasıdır.

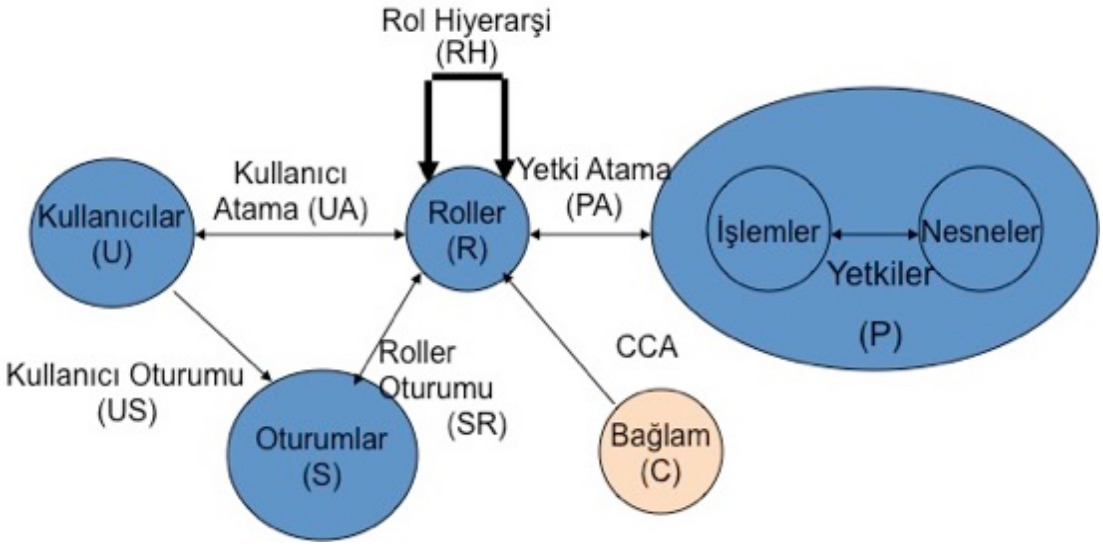
Roller	Bulunduğu Yer	Erişim Yetkileri
X_Rol	Alan1	P1,P2,P3
Y_Rol	Alan2	P4
Z_Rol	Alan3	Ø

Çizelge 2.3 SRBAC Erişim Yetkileri Belirleme Listesi [53]

2.4.1.3 Dinamik Rol Tabanlı Erişim Kontrolü Modeli

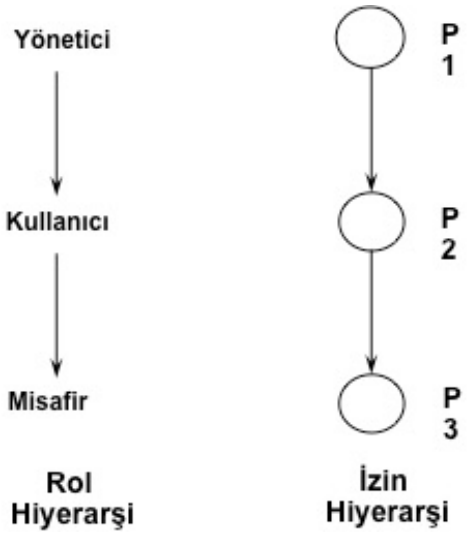
Yukarıda incelenen modellerin ortak yönleri, kullanıcının erişim isteği sırasında bağlam bilgileri büyük rol oynamaktadır. Kullanıcının nesneye erişim isteği yapıldığında, istenilen nesneye erişim izni verilip verilmediğini belirlemek için kullanıcının bağlam bilgisini sistem tarafından değerlendirme sürecine gerçekleştirilir. Erişim isteği yapıldığı andan itibaren bağlam bilgisinin değerlendirilme işlemi başlar ve kullanıcıya erişim yetkisi verildikten sonra tekrar değerlendirme işlemi gerçekleşmez. Ayrıca, bağlam bilgisi olarak zaman ve yer etkenleri kullanan ST (Spatio-Temporal) modeller, zaman ve yer gibi bağlam bilgileriyle sınırlı kalmaktadır. Dağıtık bir bilgisayar ortamında kapsamlı erişim denetim modeli oluşturulması için her türlü bağlam bilgileri ele alınmalıdır.

Bu sorunların çözümü için G.Zhang [52] tarafından Dinamik Rol-Tabanlı Erişim Kontrol (Dynamic Role-Based Access Control - DRBAC) modeli önerilmiştir(Şekil 2.17).



Şekil 2.17 Dinamik Rol-Tabanlı Erişim Modeli [52]

Bu modelde, kullanıcı bağlam bilgisine dayanılarak, rol ve yetki belirleme işlemleri dinamik olarak düzenlenmektedir(Şekil 2.18).



Şekil 2.18 Rol ve İzin Hiyerarşisi [52]

Bu amaçla DRBAC iki durum makinesi kullanmaktadır: bunlar sırasıyla kullanıcıya rolün dinamik olarak atanma işleminin yerine getirilmesi için durum makinesi ve dinamik izin atama işleminin yerine getirilmesi için ise izin durum makinesidir. Roller ve izinler hiyerarşik yapıda olup, geçiş politikalarından oluşmaktadır. Rol geçiş politika örneği Çizelge 2.4'te XML biçiminde rolün değişim süreci verilmiştir. Bu politikaya göre, "ahmet" öznesi güvensiz iletişim hattı üzerinden geldiğinde "super-user" rolü "general-user" rolüne değiştirilmektedir.

```
<ROLE_TRANSITION>
<POLICY>
<SUBJECTID>ahmet</SUBJECTID>
<BEGIN_ROLE>Super-User</BEGIN_ROLE>
<EVENT>Unsecure Link</EVENT>
<END_ROLE>General-User</END_ROLE>
</POLICY>
</ROLE_TRANSITION>
```

Çizelge 2.4 Rol Geçiş Politika Örneği [52]

Fakat bu süreçte kullanıcıya rol atama işlemi için rol hiyerarşisini denetleyen ve yöneten "Merkezi Yetki" (Central Authority - CA) düzeneği kullanılarak her türlü bağlam bilgisi elde edilmektedir. Buna göre CA, bağlam bilgilerine dayanılarak rolleri gözlemleme ve değiştirme işlemleri için kullanıcının cihazı içinde aygıt durumunu temsil eden bir "agent" aracı kullanmaktadır. Yani, her durum bir rol temsil etmekte ve mevcut durumdan başka duruma geçiş yapılarak, mevcut rol ile diğer rol arasında geçişi sağlanmaktadır. Bu eylem bağlam bilgisine dayanılarak gerçekleşmektedir.

Önerilen DRBAC modeli temel olarak RBAC modelinin kavramlarını içerir ve bunlar biçimsel olarak aşağıdaki şekilde ifade edilebilir:

- U,R,P,S,C – sistem, kullanıcılar, roller, yetkiler, oturumlar ve bağlam bilgi küme varlıklarından oluşmaktadır;
- $PA \subseteq P \times R$ - rollere yetki atama, çoktan-çoğa ilişkisine sahip;
- $UA \subseteq U \times R$ – kullanıcıya rol atama, çoktan-çoğa ilişkisine sahip;
- $RH \subseteq R \times R$ ($r1 \geq r2$ – r1 yetki izinler r2 tüm yetki izinlerini de kapsar);
- Kullanıcı: $S \rightarrow U$;
- RBAC0: Roller $S \rightarrow 2^R$,

  $$R(s) \subseteq \{ r \mid (U(s), r) \in UA \}, \quad PA(s) = \bigcup_{r \in R(s)} \{ p \mid (p, r) \in PA \};$$

- RABC1: Roller $S \rightarrow 2^R$, $R(s) \subseteq \{ r \mid \exists r' [(r' \geq r) \& (user(s), r') \in UA] \}$,

  $PA(s) = \bigcup_{r \in R(s)} \{p \mid \exists r'' [(r \geq r'') \& (p, r'') \in PA] \};$

- CC – Bağlam kısıtları CCA ⊆ CC x R – rolü belirleme için CC kümesi, çoktan-çoğa ilişkisine sahip;

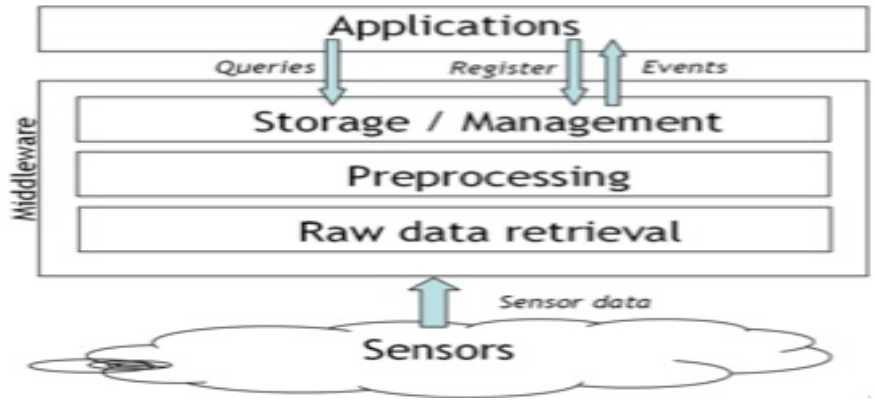
DRBAC modelinin eksik yönlerinden biri, kullanıcının cihazları her rol için durumsal aygıt rolüne sahip olması gibi oldukça karmaşık uygulama yapısı gerektirmesidir. Sistem üzerinde rollerin sayısı yükseldikçe, sistem daha karmaşık hale gelmektedir. Böylesi önemli bir sorun nedeniyle dağıtık yayın bilgisayar ortamlarında kısıtlı cihazların kullanılması gerektirmektedir.

2.5 Bağlama Dayalı Sistem için Politika-Tabanlı Mimari

Politika tabanlı sistemin ana hedefi, iyi tanımlanmış kurallarla sistemi denetlemektir. Politikalar ise sistem üzerindeki belirli bir bilgi kaynaklarına tutarlı erişim sağlayacak tanımları ifade eder.

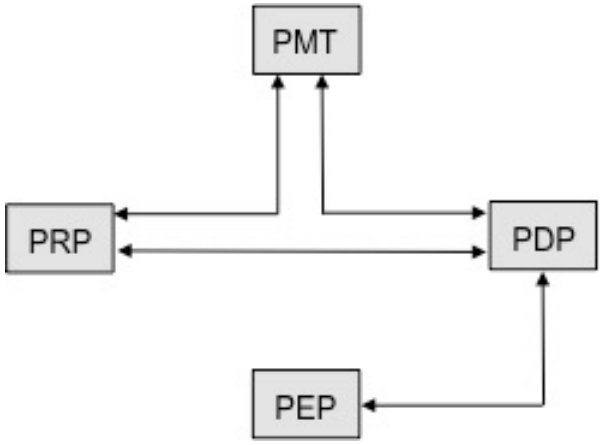
Kurallar, kendi davranışlarını yöneten her sistem için gerekli ve mevcut sistem denetimin komplikasyon etkenlerini azaltmak amacıyla sistem üzerinde politika kurallarını düzenlemelidir. Ancak bağlama dayalı bir ortamında, bağlam bilgilerinin sürekli değişmesi mevcut politikaları etkilemesi nedeniyle sistem davranış biçimi değişebilir. Böyle durumlarda politikaların değişimi ile sistem işlemlerinin dinamik denetimini sağlayacak bir mimari söz konusudur. Bu çerçevede, bağlama dayalı sistem temelindeki mimari – bağlam bilgileri esnasında politika değerlendirme durumundan sonra sistem eylem işlemini gerçekleştirir. Böylece sistemde değişen herhangi bir politika kuralı, sistem tasarımını etkilemez.

Bu sistem mimarisinin politika tabanlı ve bağlama dayalı olmak üzeri iki önemli yönü vardır. Bu anlamda, sistem mimari bileşenlerinin oluşturulması sürecinde önemli rol oynayacak ve 5 katmandan oluşan bağlama-dayalı sistemin kavramsal yapısı önemlidir(Şekil 2.19).



Şekil 2.19 Bağlama-Dayalı Sistemi [89]

İkincisi ise politika tabanlı sistem özelliğini temsil eden "politika tabanlı" yönü olup, 4 ana bileşenden oluşmaktadır [55,56]: Politika Yönetim Araçları (Policy Managment Tools - PMT), Politika Karar Öğesi (PDP), Politika Bilgi Deposu (Policy Repository Point - PRP) ve Politika Yürütme Öğesi (PEP). Şekil 2.20'da IETF kuruluşu tarafından önerilen Politika-Tabanlı Yönetim (Policy Based Managment - PBM) şeması gösterilmiştir.

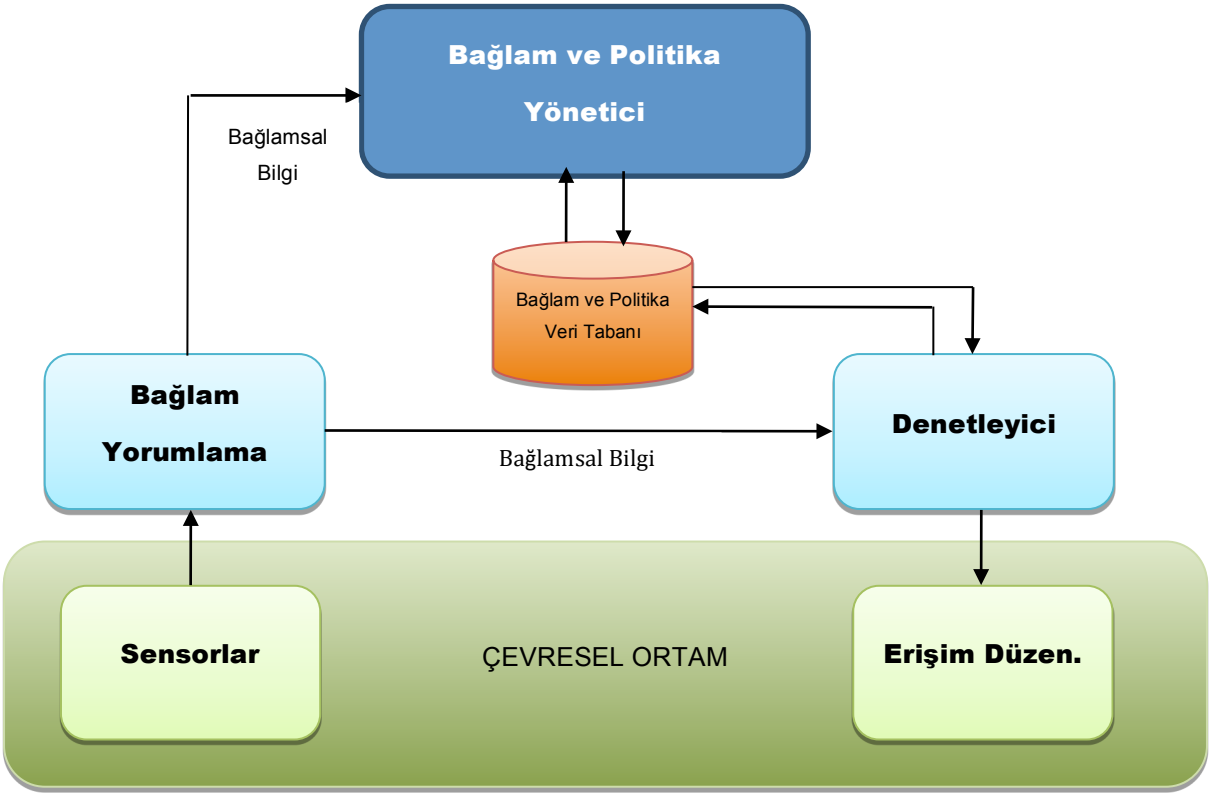


Şekil 2.20 Politika Tabanlı Yönetim Sistemi [56]

Politika-Tabanlı sistemin bileşenleri ve özelliğine sahip olan PBM, standart olarak kabul edilmektedir. H. Al-Sammarraie [54] tarafından geliştirilen mimari, işbu konuda yapılan çalışmalardan biridir (Şekil 2.21). Bu mimari işlevsel süreçlerini, "*Sensorlar*", "*Bağlam Yorumlama*", "*Bağlam ve Politika Yönetici*", "*Bağlam ve Politika Veri Tabanı*", "*Denetleyici*" ve "*Erişim Düzenekleri*" gibi altı bileşenle gerçekleştirmektedir.

Buna göre çevre ortamı kısmında (sensor ve erişim düzeneği) sistem tarafından algılanacak bağlamsal bilgilerin kaynağını temsil eder. Sensorlar,

gerekli bağlam bilgilerinin algılanmasını sağlar. Genelde bağlam bilgileri fiziksel ve mantıksal olmak üzeri iki tipe ayrılır.



Şekil 2.21 Bağlama Dayalı Sistem için Politika Tabanlı Mimari [54]

Fiziksel bağlamlar, çevresel ortama entegre edilmiş fiziksel sensorlar katmanını temsil eder. Çevresel durumların sürekli değişim bilgilerini alabilmek için bu bağlamın devamlı güncellenmesi gerektirmektedir. Mantıksal bağlam ise daha çok soyut bilgi kapsar (Sanal sensorlar: kullanıcı, grup, bilgisayar, ağ profilleri, kullanıcı etkileşim işlemleri v.s.). Mantıksal bağlam bilgileri, çevre ortamında gerekli değişikleri ifade eder.

Bağlam yorumlama, sensorlardan elde edilen ham bağlam verileri yorumlayarak, bağlam kayıtlarını oluşturmakla yükümlü olan sistem bileşenidir. Burada $PARAMETER_m$ $(1 \leq m \leq N)$ biçiminde bağlam kayıtları oluşturulması söz konusudur. Örneğin: (KullanıcıID, Yer, Zaman).

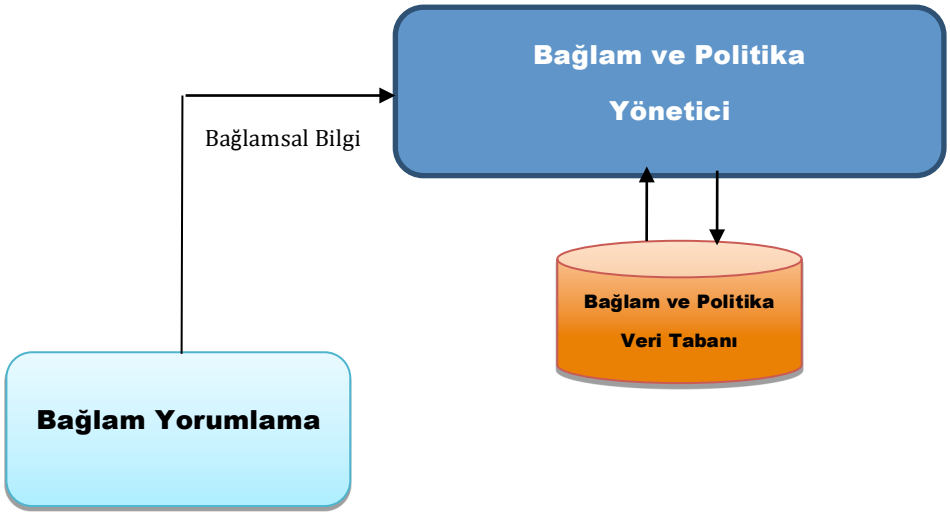
Bağlam kayıtlarının oluşturulma süreci iki aşamadan geçer ve bu iki süreci "*Yorumlama Motoru*" ve "*Kayıt Oluşturma*" olmak üzeri iki bileşen aracılığıyla gerçekleşir. "Yorumlama Motoru" - aldığı bağlamın tutarlı olup olmadığını denetler. Sensorlardan gelen veri tutarlı bir bağlam ise "kayıt oluşturma"

bileşenine iletir. Aksi durumda, “yorumlama motoru” anlamlı ve tutarlı bağlam bilgilerin üretebilmek için iki veya daha fazla bağlam verisini birleştirerek birleştirme/toplama işlemini gerçekleştirir.

Bağlam ve politika yönetici(yönetim katmanı), politika tabanlı bağlama dayalı sistemin yönetim birimidir. Bu yönetim birimi iki bileşenden oluşur: *bağlam yöneticisi ve politika yöneticisi*.

Bağlam yöneticisi, bağlam bilgilerini kategorize etme, düzenleme, depolama ve yönetme işlemlerinden sorumludur. Bu bileşen, bağlam yorumlama tarafından oluşturulan bağlam kayıtları üzerinde gerektiğinde düzenleme, kategorize etme veya bağlam veri tabanına depolama işlemini gerçekleştirir. Bağlam yöneticisi süreçleri yetkili yönetici tarafınca denetlenir.

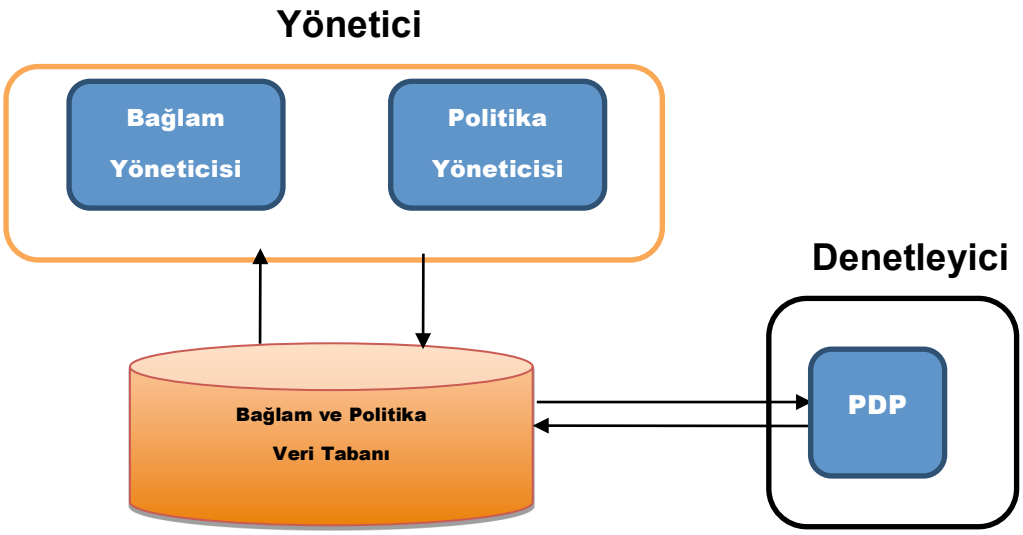
Politika yöneticisi, yönetici tarafından politikaları düzenleme, ekleme ve yönetmesini sağlayan bir arabirimdir. Sistem politika kuralları, yönetici tarafından manuel olarak eklenebilir ve güncellenebilir. Politika kuralları, politika tabanlı sistemin en önemli bileşenidir (Şekil 2.22).



Şekil 2.22 Politika Tabanlı Sistem Mimarisinin Yöneticisi [54]

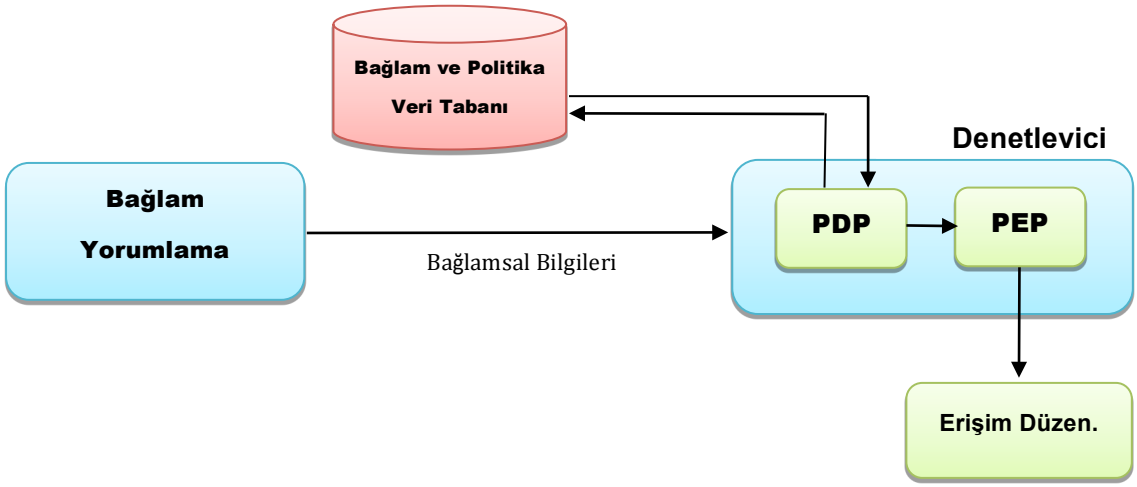
Bağlam ve politika veri tabanı, politika tabanlı bağlama dayalı sistemin ayrılmaz önemli bir parçasıdır (Şekil 2.23). Bu veri tabanı, bağlam ve politika bilgilerinin yönetici tarafından barındırılabileceği bir veri deposudur. Bu veri tabanı üzerinde sadece yetkili yönetici tarafından düzenleme, ekleme veya kurtarma işlemleri gerçekleştirilir. Aksi durumlarda, sistemdeki gizli kaynak bilgilerine yetkisiz erişim söz konusu olabilir.

Denetleyici, bağlama dayalı sistem mimarisinin politika tabanlı işlevselliği açısından en önemli bileşendir. Bu bileşen, bağlam yorumlama biriminden elde edilen bağlam kayıtları ve veri tabanında tutulan politika bilgileri üzerinde karar değerlendirme ve yürütme işlemini gerçekleştirmektedir(Şekil 2.24).



Şekil 2.23 Politika Tabanlı Sistem Mimarisinin Veri Tabanı [54]

Bu anlamda *denetleyici*, karar değerlendirmeyi gerçekleştiren ve politika eylemlerini uygulayan bir motordur. Bu motorun PDP ve PEP gibi iki önemli bileşeni mevcuttur. Aynı zamanda, politika karar verme süreci – politika kurallar durumunu değerlendirilmesi ve mevcut politika ile bağlamı eşleştirmek için durum bir politika eylemleri uygulaması gibi iki aşamalı işlemi kapsar.



Şekil 2.24 Politika Tabanlı Sistem Mimarisinin Denetleyici Bileşeni [54]

Burada PDP, politika durum değerlendirme işleminden sorumlu mantıksal bir varlıktır. PDP, *bağlam yorumlama* bileşeninden bağlam kayıt bilgilerini alır,

ayrıca ilgili politika koşulu ile uyumlu mevcut bağlamı değerlendirme işlemi gerçekleştirmek amacıyla bağlam ve politika veri tabanına tam yetkili erişimine sahiptir.

PEP bileşeni ise, PDP karar değerlendirme sürecinden elde edilen politika eylemlerini uygulama sürecini gerçekleştirir. Politika uygulama süreci, *erişim düzeneği* aracılığıyla gerçekleşmektedir. Bu mimarinin fiziksel katmanında yer alan *erişim düzeneği* ise çevre ortamı ile entegre olan fiziksel varlıklardan oluşur. Sistemin *denetleyici* bileşeninden (PEP) gelen politika uygulama sonuçlarına göre yönetilen nesneler üzerinde gerekli eylem işlemlerini uygular.

3. ARAŞTIRMA KONUSU VE YÖNTEM

Fiziksel güvenliği mantıksal güvenlikten ayrılması zor hala gelen dağıtık bilgisayar ortamıda istenilen şeffaflık, güvenlik tehdit ve saldırılara karşı sistemi savunmasız bırakması söz konusu olabilir. Fiziksel güvenlik, fiziksel media ortamında depolanan kaynak veya bilgiye yetkisiz erişimini korumak anlamını ifade eder. Aynı şeklilde mantıksal güvenlik ise sadece yetki kullanıcıların iletişim ağı üzerinde belirli bir eylemi gerçekleştirmeyi yada bilgiye erişimi temin edecek bazı önlemleri sağlamayı hedefler. Böyle açık bir dinamik ortamda yetkisiz erişim girişimlerini önlemesinde önemli olan güvenlik, gizlilik, kimlik doğrulama ve erişm denetimine gereksinim duyulmaktadır. Kullanıcı odaklı sistemler, korunan kaynak bilgiye “her yerden”, “her zaman” ve “her şekilde” şeffaf erişebilirliği kullanıcılara sunmaktadır. Kullanıcı ve veri ilişkisi, istenilen sistem kaynaklarına kolay ve şeffaf erişilebilirlik kullanıcı ihityaçlarını ifade eder.

Sonuç olarak, dağıtık bilgisayar ortamda sistem kaynaklarının koruma düzeneklerin yeterli derecede güvenli olmasına büyük önem verilmelidir. Bu bağlamda, veri şeffaflığı ile veri güvenliği arasında sıkı bir dengenin sağlayabilinmesi önemlidir. Veri şeffaflığı - açık dağıtık bilgisayar sistemlerinde kaynak bilgilerine kesintisiz erişilebilirliğini sağlar. Diğer taraftan veri güvenliği ise, sadece yetkili kullanıcıların bilgi kaynağına erişim hakkını verir. Aynı zamanda etkin ve uygulanabilir erişim denetim politikaların kullanımı büyük öneme sahiptir.

Bu anlamda, kullanıcı gereksinimleri ile sistem güvenlik kısıtları arasında hasas dengeyi sağlayacak adaptif erişim kontrol düzeneğinin önerilmesi söz konusudur. Bu tezin ana hedeflerinden biri de bu dengeyi sağlayacak çözümleri üzerinde erişim denetim sistemlerin kurgulanmasıdır.

Sağlık alanında veri güvenliği, kişisel bilgilerin gizliliği açısından çok önemlidir. İkinci bölümde belirtilen yöntemlerin zayıflıklarından kaynaklanan güvenlik açıklarının ortadan kaldırılması gerekmektedir. Bu açıkların yaşayan, dinamik bir altyapı kullanarak güncelliğini koruyan bir politika yönetimi gereksinimi vardır. Bu gereksinim bu tezin temel konusunu oluşturmaktadır.

Tez kapsamında güvenlik açıklarının ortadan kaldırılmasını amaçlayan yeni yöntem model olarak tartışılmış ve sağladığı üstünlükler teorik olarak ortaya konulmuştur. Karşılaştırma yapılırken sentez yöntemi kullanılarak ortaya konulan yöntemin üstünlükleri tartışılmaktadır. Bu anlamda bir örnek model üzerinden “her zaman”, “her yerden” ve “her şekilde” güvenli erişim isteklerini karşılayabilen durumsal bağlam bilgilerin semantik olarak yorumlayan erişim karar düzeneğinin uyarlanması söz konusudur.

4. SAĞLIK ALANI İÇİN ÖNERİLEN BAĞLAMA-DAYALI ROL TABANLI SEMANTİK YETKİLENDİRME MODELİ

Yaygın bilgi sistemlerinde (pervasive information systems) erişim kontrolü modellemesi farklı açılardan zorunlu bir görev olarak kabul edilebilir ve erişilebilirlik yaygın bilgi sistemi için anahtar bir özelliktir. Buna kullanıcı bakış açısından bakılırsa, erişim denetimi erişilebilirlik için bir engel olarak kabul edilmelidir. Çünkü kullanıcılar için her zaman ve her şekilde istenilen kaynağa erişim söz konusu olmayabilir. Aynı zamanda, sistem yöneticisinin bakış açısından yorumlandığında erişim denetimi, güvenli etkileşimlerin sağlanması ve açık ortamlarda erişilebilirlik sunarken sistemin bütünlüğünün korunması için son derece önemlidir. Bu anlamdaki hedefi karşılayabilmek için mobil, akıllı ve dinamik ortamlarda şeffaf, ama güvenli bir erişim söz konusudur.

Bir mobil uygulama ortamında kullanıcı bağlamı son derece dinamik bir yapıya sahiptir ve bir kullanıcının “kullanıcı kim” tekniğine göre kullanıcı bağlam bilgisi olmadan erişim yapılmaya çalışılması sistem güvenliğini tehlikeye atabilir. Bu anlamda, “kullanıcı nerede” ve “kullanıcının durumu ve bu durumu belirleyen çevre” konsepti temelinde kurgulanan bağlam etkenleri bir dizi erişim denetim düzeneklerinin hazır edilmesini gerektirmektedir. Sonuçta erişim kontrolünün modellenmesi, bağlamsal kısıtlamalar üzerinde karar verme sürecine doğru kaymıştır. Bu özellik, sistem kaynakları üzerinde her zaman ve her yerden daha iyi bir erişim yönetimi sunmakla beraber mobil kullanıcıların dinamik erişilebilirlik gereksinimlerini karşılamaktadır. Erişim kontrolü ihtiyaçlarına yakından bakıldığında, kurumsal düzeyde yetki atama düzeneklerinin evrimsel değişimi karşımıza çıkar. Dağıtık kaynak yönetimi, genellikle RBAC modeli kullanılarak gerçekleştirilmektedir. Yaygın ortam gibi yeni paradigmalar sonucunda, bu modelin bağlama dayalı ifade edilmesi için yeni gereksinimler de ortaya çıkmıştır. Bu çerçevede önerilen model çeşitliliğine ve zenginliğine rağmen, bağlama dayalı karar verme sürecinde kullanıcı bağlamının uygulama alanında farklı ifade ve tanımlanma işlemleri, ayrıca bağlam edinme, modelleme ve yorumlanması için birçok mevcut teknikler kullanımı zorunlu bir araştırma sorunu olarak kalmaktadır. Ayrıca ortamın dinamik konseptinin, izin atama süreçlerine de yansıyacağını dikkate

almak gerekir. Gerçek zamanlı sistemlerde izin atamanın dinamiği, sadece bağlamsal boyutta değişikliklerle ilişkili değildir. Ancak, sıkı güvenlik politikalarıyla bilgi gizliliğinin korunması için geleneksel yönetimin birçok yönü vardır.

Sonuç olarak, erişim denetimi modellemesi sadece bağlamsal dinamizm üzerinde değil, belki erişim talebinin ortaya çıktığı durumda kritik veya yaşamı tehdit eden kullanıcı durumsal konumu benimsenmelidir. Bu anlamda birçok araştırmalar, duruma dayalı karar verme sürecini kapsayan ve ortam durumuna göre kullanıcıların kaynak bilgiye erişimini sağlayacak esnek çözümleri sunabilecek uyarlanabilir erişim denetim modellemesi üzerinde yoğun çaba gösterilmektedir.

Buna rağmen yaygın bilişim veya dağıtık bilgisayar ortamlarında, birçok uygulama ve servisler için tutarlı olarak belirlenebilen bağlamlar büyük rol oynamaktadır. Bağlamsal bilgilerin oluşumunda büyük etken olan “durumsal bağlamlar” (situational contexts), sistemin bilgi kaynaklarına erişim sürecini düzgün denetleyecek erişim kontrolü politikalarının tutarlı olması için gereklidir. Erişim kontrolü politikalarının vazgeçilmez bir parçası olarak bağlamların entegrasyonu politika dillerinin özelliğine bağlı olarak çeşitli yollarla gerçekleştirilebilir. Bu süreç kapsamında, bağlamların anlamsal yönetilmesi ve politikada kullanılması arasında bir ayrım yapılması gerekir. Bu ayrım yönetim açısından esnekliği veya politikaları yeniden yazmadan bağlamların anlamlarını değiştirmeyi sağlar.

Bağlama dayalı sistemlerde, politika belirleme sürecinin dinamik bir ortama uyumlu olması gerekmektedir. Durumsal bağlamları belirleyen ortam dinamik bir ortam olarak tanımlanabilir. Durumsal bağlamlar oldukça değişkendir. Ortam üzerindeki varlıklar o anki bir veya daha fazla bağlamlarla ilişkilendirilebilir. Bunun sonucu olarak varlıklar ve bağlamlar arasındaki ilişkilendirme sürecinin mümkün olan her tür örnekleme için politikalar yazmak olanaksızdır. Bu nedenle, sistemin anlayabileceği biçimde bir politika yazılması gerekmektedir. Başka bir deyişle, durumsal bağlamları semantik olarak anlayıp, yorumlayabilen politika sistemlerine ihtiyaç duyulur. Bu tür erişim kontrolüne, semantik duyarlı/dayalı erişimi kontrolü denilmektedir.

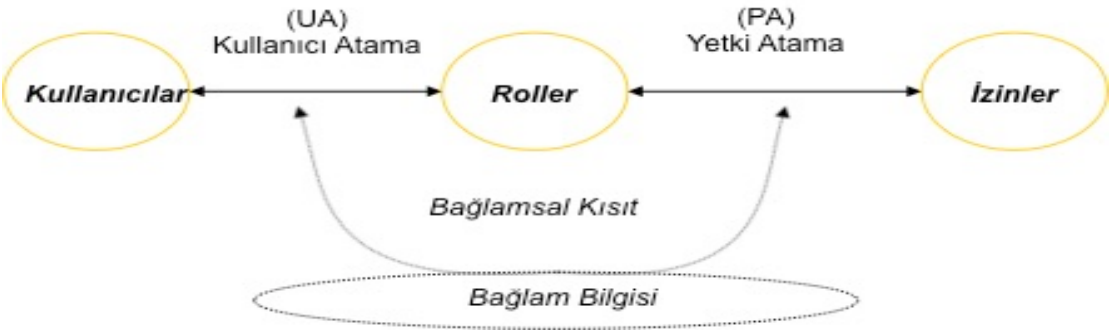
Bu bölümde, bağlama dayalı rol ve izin atama teknikleri, ayrıca duruma dayalı izin atama düzeneğini kapsayan bir RBAC modeli ele alınarak, anlamsal bağlam modelleme yaklaşımıyla elde edilecek bağlam bilgilerini anlamsal tabanlı bir politika üzerinde kullanan bir yetkilendirme modelinin kurgulanması söz konusudur.

4.1 Bağlama-Dayalı RBAC Modeli

Dağıtık bir ortamda, yetkilendirilmiş bir kullanıcıya erişim hakkı sağlayan erişim denetim düzenekleri önemli bir faktör haline gelmiştir. 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 erişmektedir.

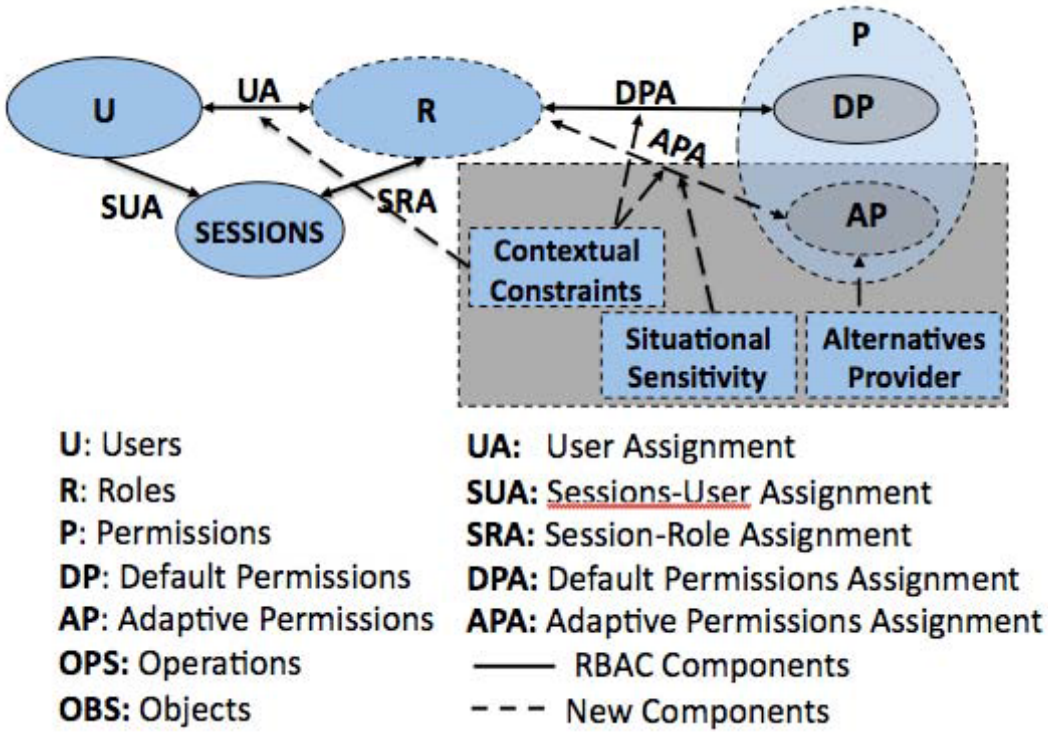
Bağlama dayalı erişim kontrolü modellerinin birçoğu RBAC ve ABAC modellerine dayanmaktadır. RBAC modelinde, öznelerin roller aracılığıyla temsil edilerek erişim denetim süreci gerçekleştirilmektedir. ABAC modelinde ise yetkilendirme karar sürecini özne, kaynak ve çevresel varlıkların özniteliklerine dayanılarak gerçekleştirilmektedir. Bu öznitelikler, kurum rolleri gibi statik ve yer konumu gibi dinamik olabilmektedir. Ancak ABAC modeli yaklaşımında politikaların tanımı ve yönetimi oldukça karmaşıktır. Aynı zamanda, varlıkların öznitelikleri olarak benimsenen kavram aslında bağlam bilgileri olarak düşünülebilir.

RBAC ve ABAC erişim denetim düzeneklerinin ortak amaçları kaynakların ve öznelerin temsil gücünü, geliştirilen model çerçevesinde zenginleştirmektir. Fakat bu tür zenginleştirme çalışmaları öznelerin ve kaynakların anlamsal olarak temsil edilmesini sağlayamamaktadır. Bu çerçevede, hem RBAC modelindeki role göre yetkilendirme, hem de ABAC modelindeki varlıkların özniteliklerine göre yetkilendirme özelliklerini kapsayan başka bir model üzerinde semantik bağlam yaklaşımının kurgulanması gerekir.



Şekil 4.1 CAAC-RBAC Modeli [90]

Bağlama dayalı erişim denetim modelleri, bağlam bilgileri kullanılarak erişim denetim sürecini gerçekleştiren düzeneklerdir. Bir çok bağlama dayalı erişim denetim modelleri, yeni bağlamsal kısıtlar yaklaşımlarıyla genişletilmiş RBAC (Context-Aware Access Control - CAAC) modeline dayanır (Şekil 4.1). Bu modellerde, kullanıcıya rol atama ve rollere yetki atama işlemleri bağlamsal kısıtlar üzerinde gerçekleşmektedir. Bu mantıkla genişletilmiş RBAC modelinde esnek bir yetkilendirme ve kullanıcıların ihtiyaçlarını karşılayabilecek uyarlanabilir (adaptive) izin düzeneğinin oluşturulması hedeflenmektedir.



Şekil 4.2 Referans PS-RBAC Model [72]

Böylece, bağlamsal kısıtlar üzerinden kullanıcı atama (UA – User Assignment) ve izin atama (PA – Permission Assignment) işlemleri dinamik olarak gerçekleştirilecek yeni bir erişim denetim düzeneği ortaya konmaya çalışılmaktadır.

Bu tezde PS-RBAC (Pervasive Situation-Aware Role-Based Access Control) modeli referans modeli olarak kullanılmaktadır(Şekil 4.2). Bu modelde, kullanıcıların (U) rollere (R) atama veya eşleştirme işleminden sonra rollere ait farklı izinler söz konusu olabilir. Bu izinler iki tipten oluşabilir: varsayılan ve uyarlanabilir yetki izinleri. Buradaki adaptif izinler (AP) işleminde, önemli acil durumların kullanıcının erişim hakkı verilmediği senaryosunda alternatif bir kaynağa erişim izin hakkı tanınmaktadır.

Bu referans PS-RBAC modelde [72] yer alan bileşenler ve aralarındaki ilişkileri açıklayan biçimsel tanıma bir göz atalım. Bu tür modellerde kullanıcı roller, kullanıcı, izin atamaları ve bağlamlar arasında UA, PA ve CA olmak üzere üç farklı ilişki söz konusudur.

Tanım 1 (Kullanıcı) U kullanıcılar kümesi ve $u_i \in$ U kullanıcı olsun. Her bir {u_1, u_2, u_3, ... ,u_n} kullanıcı için çeşitli {r_1, r_2, r_3, ... ,r_m} roller atanır.

Tanım 2 (Rol) R roller kümesi ve $r_i \in$ R rol olsun. Her bir {r_1, r_2, r_3, ... ,r_m} rol için çeşitli {p_1, p_2, p_3, ... ,p_n} izinlerin eşleştirme işlemi yapılır.

Bu modeldeki kullanıcılar, sistem ile etkileşim içinde olan bir özne varlığıdır. Bu özne, bir bilgisayar sürecini, bir web servisini ya da erişimi denetlenen veya rol ataması yapılacak bir aktif varlıktır. Her bir kullanıcıya çeşitli roller ve her bir role birçok kullanıcılar atanabilen çoktan-çoğa bir ilişki mevcuttur. Aynı şekilde, her bir role birçok izin ve her bir izine birçok rolün atanabildiği çoktan-çoğa bir ilişki söz konusudur. Rol (R), bazı yetki izinlerinin alınması ve işlemleri yürütmek üzere bir kullanıcı ile ilişkilendirilen kurumsal bağlamdaki bir pozisyondur. Roller, önceden tanımlanmış bazı semantik yapılar ve bağlamlara göre kullanıcılarla ilişkilendirilmektedir.

Kullanıcılar ve roller arasındaki eşleşme tanımları oturumlar kümesi üzerinde yapılmaktadır. Bir kullanıcı sisteme giriş yaptığında kullanıcı bir veya bir kaç role eşleşme işlemini oturumlar üzerinde gerçekleştirir. Buna göre, sistemde

belirli bir görevi gerçekleştirmesi için ihtiyaç duyulan minimum rollerin kullanıcıda aktif hale getirilmesidir.

Kullanıcı ve rollerin eşleştirme süreci, “Session User Assignment” (SUA) ve “Session Role Assignment” (SRA) olmak üzeri iki ana işlev aracılığıyla gerçekleştirilmektedir. SUA, kullanıcı ve oturum sayısı arasındaki birden – çoğa eşleşme ilişkisini (SUA: S x U) ifade eder. SRA, oturum sayısı ile roller arasındaki çoktan - çoğa ilişkiyi (SRA: S x R) tanımlar.

Tanım 3 (Bağlam) C tüm bağlamları içeren bir küme ve $C_i \in C$ bağlam olsun.

C_i = < C_Adı, C_Attr > ve C_Attr = < adı, tip, değer > =>

C_i = < C_Adı, (adı, tip, değer) >;

Bağlam, kullanıcının bulunduğu yeri, oda ısısı veya erişim zamanı gibi ölçülebilir/tanımlanabilir durumsal bilgiyi temsil eder. Bu modelde bağlam, bağlam ismi ve bağlam nitelikleri içerir. Bununla beraber, bağlam nitelikleri – bağlam niteliğinin ismi, tipi ve değerleri üçlüsünden oluşur.

Örneğin:

C_1 = < Location, (Hastane, String, Acil) >;

C_2 = < Time, (Pazar, Integer, 0230) >;

Tanım 4 (Bağlam Tanımı) CD, bağlam tanımlarını içeren bir küme ve $CD_i \in CD$ bir bağlam tanımı olsun.

CD_i = < EntityID, $\{C_1 \cap C_2 \cap C_3, \ldots \cap C_n\}$ >;

Bağlam tanımı (CD) çeşitli bağlamları içerir ve EntityID bağlamları arasında ilişkiyi tanımlayan bir varlıktır. Bu anlamda EntityID varlığı, özne veya nesne olabilir. Örneğin: CD_1 = < Doktor, $\{C_1 \cap C_2\}$ >;

Tanım 5 (Bağlam Kısıtı) Diyelim ki, CC ihtiyaç duyulan bağlamların kümesi ve $CC_i \in CC$ ihtiyaç duyulan bir bağlam kısıtı olsun.

CC_i = $\{CCE_1 \cap CCE_2 \cap CCE_3, \ldots \cap CCE_n\}$;

Burada. CCE_i = < CD_i , CN >, CN = {+/-};

Tanım 6 (Kullanıcı Atama) UA, kullanıcı atama işlemi olsun. Her bir U={u_1, u_2, u_3, ... ,u_n} kullanıcılar ile çeşitli R={r_1, r_2, r_3, ... ,r_m} roller arasındaki eşleştirme ilişkisi,

$UA \subseteq U \times R \times CC$;

$UA_i = < u_j, r_k,$ Yetki_Aktarma_Durumu>;

Tanım 7 (İzinler) P, kaynak veya nesneler üzerinde bir takım işlemlerin gerçekleştirilmesi için erişim türünü belirleyen izinler kümesi ve $p_i \in P$ izin olsun: O zaman nesneler ile eylem işlemleri arasındaki ilişkisi,

$P = 2^{AxO}$;

$p_i = <O, A>$;.

Burada O bir nesne veya sistem kaynakları, A ise (read, write, update, v.s) eylem işlemlerini ifade eder. Nesneler ile bu eylem işlemleri arasında karşılıklı ilişki söz konusu olup, bir işlem bir ya da birçok nesne üzerinde gerçekleşebilir. Aynı şekilde, bir nesneye farklı izinler ilişkilendirilebilir.

Tanım 9 (İzin Atama) P varsayılan izin olsun.

$PA \subseteq R \times P \times CC$;

$PA_i = < r_j, p_k, CC_i >$;

Varsayılan izinler (DP), sistem yöneticisi tarafından açıkça tanımlanmış temel izinleri belirler.

Bağlam kısıttı (CC), mevcut bağlama göre UA ve PA işlemlerinin dinamik olarak gerçekleşmesi için gereklidir. Bu kapsamda, uygun bir CC oluştuğu zaman UA ve PA işlemleri gerçekleşir.

Bu modelin biçimsel tanımı aşağıda belirtilmiştir:

- U,R,P,S,C;
- UR(kullanıcı rolleri) – geleneksel RBAC olduğu gibi kullanıcı rolleri ifade eder;
- S (oturumlar) – her oturum sırasında kullanıcı için bir rol atanır. kullanıcı ve bağlam roller arasında eşleşme yapılarak, atama süreci gerçekleştirilir;

- user_sessions (u : U) → 2^S;
- session_roles (s : S) → 2^R; R(s) ⊆ { r | (U(s), r) ∈ UA
- UA ⊆ U × R × CC.
- R → 2^U, assigned_users (r)=U | (u,r) ∈ UA;
- PA(s)= $\cup_{r \in R(s)}$ { p | (p, r) ∈ PA };

  PA ⊆ R × DP × CC;
- assigment_permissions (r : R) → 2^P;

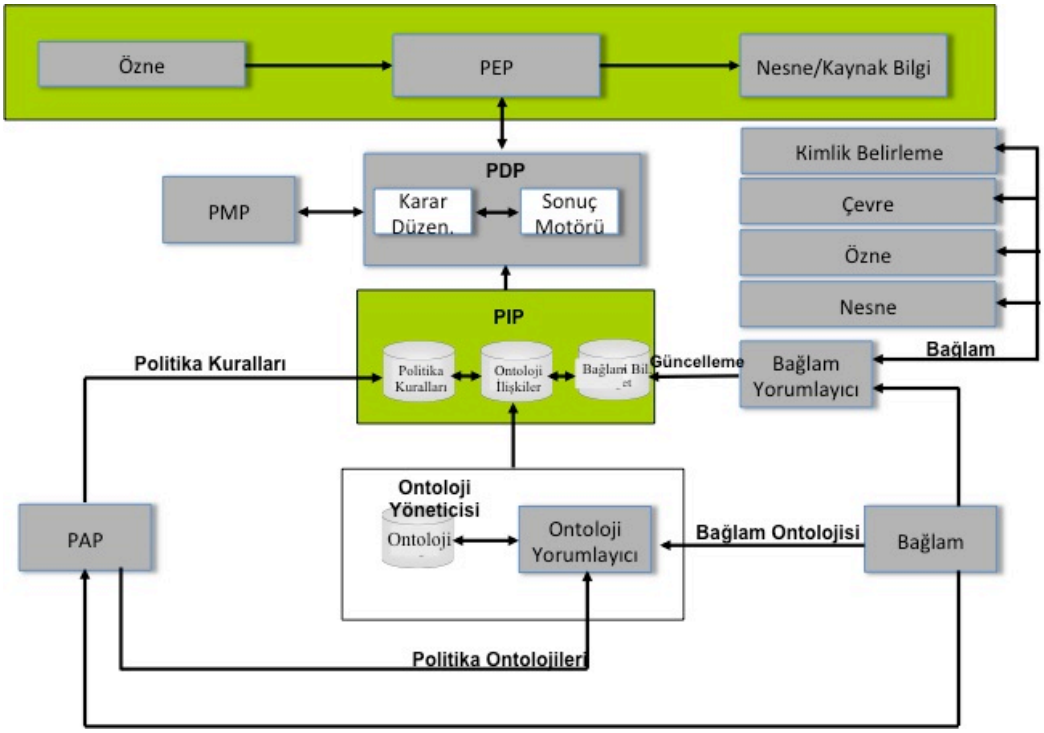
Burada söz konusu olan, bu referans modelin, herhangi bir bağlama odaklı politika modeli yaklaşımına uyarlanarak, kaynak bilgiye erişim gereksinimi duyan varlıklar ve kaynak bilgileri üzerindeki izin yetki işlemleri arasında arabulucu rolüne sahip olan bağlam odaklı yaklaşımını ortaya koymaktır. Bu yaklaşım, kaynak bilgi sahibi, kullanıcı ile kaynak sahibi arasındaki ilişki, varlıkların durumsal bilgisini içeren anlamsal bir bağlam modellemesi üzerinde yetki izinlerini tanımlayan bağlama dayalı erişim denetim çözümünün uyarlanması söz konusudur. Erişim denetimi üç tip bağlama göre gerçekleştirilmektedir.

1. Özne bağlamları (subject contexts - SC) – özne, nesne veya kaynak üzerinde eylem gerçekleştiren bir varlıktır. Özne bağlamları, nesne veya kaynak üzerinde erişim hakkı elde etmek için öznenin özelliklerini tanımlayan bilgidir. Bu anlamda özne bağlamları, bir varlık tarafından istenmesi durumunda, erişim ayrıcalıkları için erişim haklarının tespit edilmesi amacıyla kullanılır. Özneye dayalı bağlamlar, özne rolü, kimlik tanımı, kimlik kanıt bilgileri, adı, görevler, servisler, aygıtlar v.b. gibi unsurları içerir.
2. Nesne bağlamları (object contexts - OC) – nesne, öznenin üzerinde işlem yaptığı bir varlıktır. Nesne bağlamları, erişim denetimi karar verme sürecini etkileyen bilgiler olup, korunan nesnenin o anki durumu ve erişim denetimi kararlarını gerçekleştirmesi için ilgili durumu karakterize etmek üzere kullanılan nesneye dayalı bilgiler.
3. Çevre bağlamları (environment contexts - EC) – işlem gerçekleş-tiğinde oluşan ortamın durumunu belirler. EC, erişim kontrolü

politikalarının uygulanmasında etkili olan, ancak özne veya kaynak ile ilişkili olmayan tarih, saat, ısı gibi bağlamsal bilgilerdir.

Yetkilendirme karar süreci tüm bağlamları değerlendirir ve erişim hakları elde etmeye çalışır. Bu tezde önerilen SCA-RBAC (Semantic Context-Aware – Role Based Access Control) modelin yetkilendirme mimarisi Şekil 4.3'te verilmiştir. Buna göre mimari altı önemli bileşenden oluşmaktadır:

1. Ontoloji Yöneticisi – özne, nesne, eylem ve politika etki alanındaki ontoloji bilgilerin toplanması ve güncellenmesi işlemi gerçekleştirmektedir ve varlıklar arasında semantik ilişkileri düzenlemektedir.
2. Bağlam Yöneticisi – çevresel ortamda bağlam bilgileri elde ederek, bilgi tabanı üzerinde bağlam bilgilerin güncellenmesini yapar.
3. Bilgi Tabanı – etki alanı ontolojisinin veri deposudur. Burada güvenlik kuralları kümesini, yaklaşımlar arasında ilişkileri ve doğrudan bağlam bilgileri barındırır.
4. Politika Uygulama Birimi – erişim istekleri alması ve erişim kontrolü uygulamak için kullanılır. Yetkilendirme kararı elde etmek için istekte bulur ve bu kararın uygulanmasını gerçekleştirir.
5. Politika Karar Birimi – uygulanabilir politikaları değerlendirme işlemi yapar ve mevcut bağlam, kurallar ve duruma dayanarak yorumlama motoru düzeneği ile yetkilendirme kararı (izin veya red) süreci gerçekleştirir. PDP, erişim kontrolü mimarisinin çekirdek bileşenidir. Aynı zamanda erişim isteği, bir S öznenin O nesne üzerinde C bağlamsal bilgi temelinde A eylemi gerçekleştirme anlamıyla eşdeğer (S,A,C,O) olarak modellenebilir. Başka bir deyişle PDP, karar verme ve yorumlama gibi iki parçadan oluşan bir politika yürütme motorudur. Bu anlamda, mevcut durumsal bağlam göre erişim isteği üzerinde karar verme ve yorumlama düzenekleri politika kuralı ve bağlamsal bilgileri elde etmek için bilgi tabanı ile iletişim kurar.
6. Politika Yönetimi Birimi - politika veya politika kümesi yaratılması işlemi gerçekleştirir.



Şekil 4.3 Bağlama-Dayalı Erişim Kontrolü Mimarisi

Bu SCA-RBAC modelin biçimsel tanımı aşağıda belirtilmiştir:

$M = \{S, O, E, A\}$

- S – kaynak bilgisine ulaşmak isteyen özne varlığı;
- O – özne varlığının üzerinde eylemi gerçekleştirecek nesne veya kaynak varlığı;
- E – erişim denetimi karar sürecini etkileyecek koşul veya çevresel durum;
- A – Öznenin nesne üzerinde gerçekleştireceği eylem işlemleri;
- $SCk\ (1 \le k \le K)$, $OCm\ (1 \le m \le M)$, $ECn\ (1 \le n \le N)$ - özne, nesne ve çevre varlıkları için bağlamlar;
- C(s), C(o), C(e)- özne, nesne, çevre için bağlam eşleşme ilişkileri:

  $C(s) \subseteq SC1 \times SC2 \times ... \times SCk;$

  $C(o) \subseteq OC1 \times OC2 \times ... \times OCm;$

  $C(e) \subseteq EC1 \times EC2 \times ... \times ECn;$
- S öznenin O nesne veya kaynağın hangi bilgi kısmına ve hangi E koşullar altında erişebildiğini tespit ederek, eylem gerçekleştirmesi ile ilgili politika kural:

  $f(C(s),C(e)) \rightarrow Access\ (s,o,e.a)$

4.2 Bağlamın Yorumlanması

Bir yetkilendirme düzeneğinin karar verme sürecinde, bağlama dayalı rol ve izin atama olmak üzere iki tür bağlama dayalı eşleşme işlemi gerçekleştirilmektedir.

Bağlama dayalı rol eşleştirme süreci kolaylaştırılarak, rol atama işlemleri zenginleştirilebilir. Bu modelde, rol eşleştirme işlemi için ihtiyaç duyulan bağlamsal nitelikleri, sistem gereksinimlerine göre yönetici tarafından verimli şekilde tanımlanabilir ve güncellenebilir. Sonuçta, uygulama etki alanı ihtiyaçlar doğrultusunda bağlamsal nitelik açısından kişiselleştirilebilir ve mevcut bağlamsal bilgilerin nitelikleri üzerinden rol eşleşme işlemi gerçekleştirilebilir. Örneğin: Sağlık etki alanı ile ilgili bağlamsal bilgiler aracılığıyla acil binasına giriş yapan doktorun yeri tespit edilerek, ona “Acil_Dr” rolünü otomatik atama işlemi gerçekleştirilebilir. Uygulama alanı ihtiyaçlarına göre, konum yer bilgisi farklı düzeylerde ve farklı türde yorumlanabilir. “Genel konumu” (GPS koordinatı), bulunduğu belirli yer ile ilişkili “özel konumu” (RFID kart veya diğer kimlik doğrulama düzeneklerin uygulandığının tespiti) ve belirli nesnenin kullanıcının bulunduğu yerin tespit edilmesinde yardım etmesi gibi “oransal yakınlık” (Doktorun, hasta yatağına yakın bir yerde bulunması) bağlamsal bilgilere göre rol eşleştirme işlemi gerçekleştirilir.

Benzer bir hiyerarşi zamansal bilgilere göre de uygulanabilir. Genel zaman şeması, kullanıcının sisteme eriştiği zaman tanımlanabilir. Özel zaman şeması, “Klinik_Dr” rolü olarak sisteme erişen doktorun çalıştığı zaman aralıkları olarak özel olarak ifade edilebilir ya da bir hemşireye “İlaç_Servisi” rolünü alma yetkisinin verilmesi gibi olay veya eylemin cereyan ettiği zaman ile ilgili olan “Oransal Zamanlama”. Özellikle otomatik ilaç dağıtımı sistemlerinde durum öyledir. Bağlam tabanlı rolün özellikleri sadece bilgi kaynağına erişimin sağlanması için değil, güvenlik koruma adımı olarak mevcut rolün değiştirilmesi veya iptal için kullanımı şeklinde de söz konusu olabilir. Ayrıca kullanıcının bağlamsal nitelikleri, kullanıcının profili ve bulunduğu yere göre görev atama işlemi için kullanılabilir. Örneğin, bir hasta bazı komplikasyon durumlarıyla karşı karşıya kaldığı ve bir doktorun acilen müdahalesini gerektiren durumda, sistemdeki hasta kayıtları üzerinde işlem yapabilen rolün hasta ile ilgilenecek en yakın sağlık personeli kullanıcısına atama işlemi gerçekleştirilmesi gerekir.

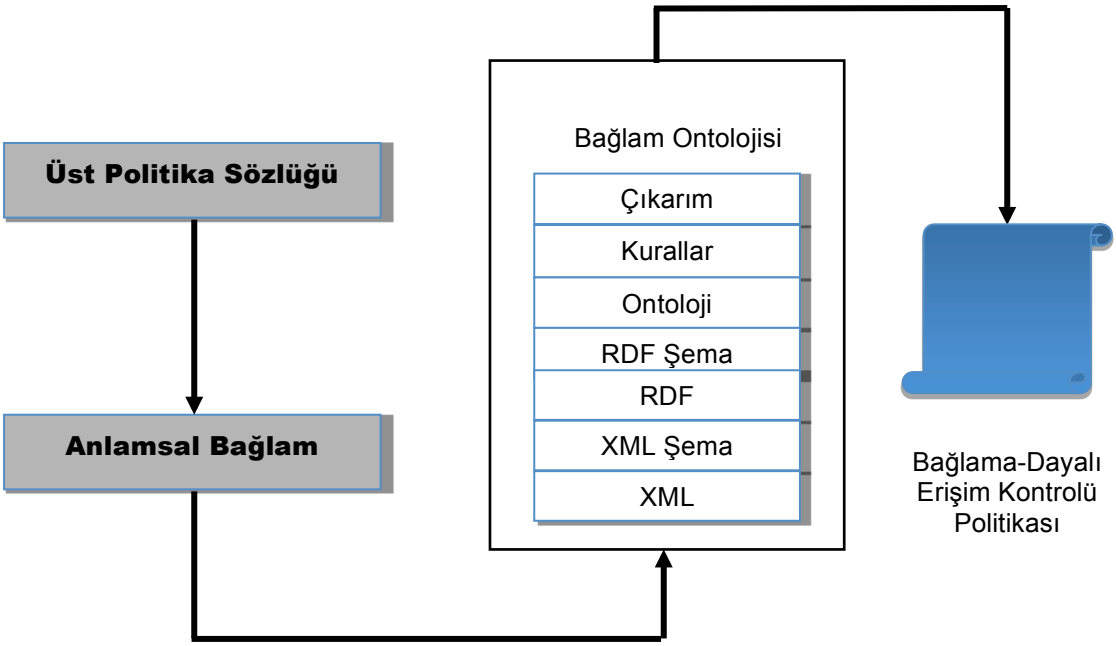
Aynı şekilde bağlama dayalı izin eşleştirme sürecinde de, önceki örnekte belirtildiği gibi bir doktorun acil bir durum bağlamında hasta kayıtlarına erişim izni elde edebilir. Ayrıca bu modelin en önemli bileşeni duruma göre sistemin karar verme yeteneğine sahip olmasıdır. Durum algılama mekanizmaları genelde, durumu tanımlayan mantıksal bağlamsal değerleri üzerinden durumun tespiti için tümdengelim (deductive) yöntemleriyle veya ontolojiler üzerinden anlamsal benzerlik sınıflandırması yapılarak çalıştırılmaktadır.

4.2.1 Semantik Bağlam Modellemesi

Bağlam, aslında, herhangi bir varlığın bir özelliğini belirler ve bağlam bilgilerinin sürekli değişmesi sonucunda mevcut politikaları etkilemesi nedeniyle sistemin davranış biçimi değişebilir. Bu nedenle erişim denetim politikaları semantik bağlam bilgileriyle entegre edilerek, erişim denetimi düzeneği içerisinde yer alan özne, kaynak ve eylemlerin anlamsal olarak temsil edilmesi gerekmektedir.

Bağlam modelleme, tüm varlıkların özelliği ve bir bütün olarak bağlamı tanımlamak için gerekli olan varlıklar arasındaki ilişkileri belirlemektir. Bağlam modellemenin amacı, üst seviye varlıklar kümesinin modellenmesi ve farklı uygulama alanlarındaki özel kavramları eklemek için esnek genişletilebilirliği sağlamaktır. Bu kapsamda, bağlam modelinin ontoloji tabanlı gösterim üzerine uyarlanması söz konusudur. Şekil 4.4'te bir üst politikadan bağlamın nasıl elde edildiği süreci verilmiştir.

Üst politikalar, politikaların yorumlanması ve çelişkilerin çözümlenmesi ile ilgili politikalardır. Bu anlamda sistemin davranış biçimini belirleyen politikaların tanımlanmasında bağlam ontolojisi önemlidir.



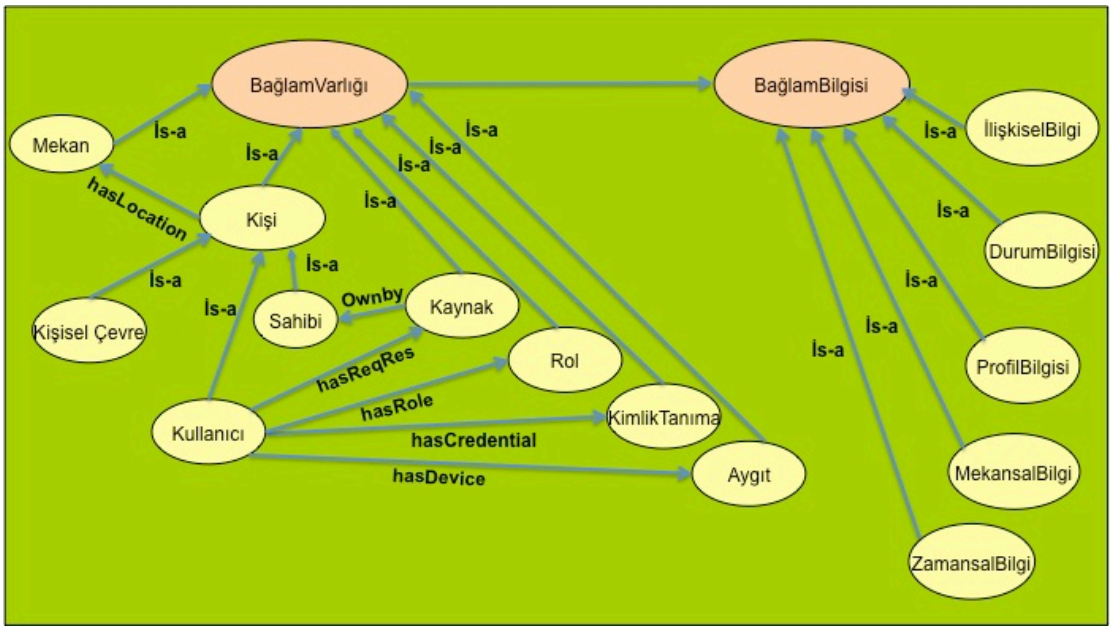
Şekil 4.4 Bağlama-Dayalı Erişim Kontrolü Politika Oluşturma Süreci [62]

Ontoloji, bir bilgi alanını tanımlaması ve temsil etmesi için kullanılan ortak terimleri ve kavramları bünyesinde barındırır. Ontoloji kapsamındaki bu terim setleri (bağlamlar), erişim denetim politikasındaki kuralların oluşturulmasında kullanılır. Bu anlamda, anlamsal web dilleri aracılığıyla bağlam ontolojisinin oluşturulması gerekmektedir. Buna göre - politika sisteminde işlenebilmesini sağlayacak, biçimsel bağlam terimleri tanımlanmalı, ayrıca diğer sistem veya uygulamalar için kolayca paylaşılabilir ve sistem işleyişini olumsuz etkilemeden yeni bağlam uygulanabilir olmalıdır.

Dağıtık bir ortamda bağlam gösterim şekli çok önemlidir. Çünkü bağlamların, çevre ortamındaki varlıklar arasında entegre bir şekilde ilişkilendirilmesini ve kullanılmasını gerektirir. Başka bir deyişle, erişim denetimi politikalarında kullanılacak bağlamlar gerektirir. Genelde bağlamların modellenmesinde veri tabanı şema, XML, UML gibi diğer yaklaşımlar kullanılmaktadır. Ancak, bu yaklaşımlar OWL gibi anlamsal web dilleriyle karşılaştırıldığında anlamlılık açısından yoksul kalmaktadır. Bu ise anlamsal web dillerinin bağlam modellemede yaygın kullanılmaya başlamasının temel nedenidir.

4.2.2 Bağlamsal Terim Gösterimi

Ontolojide tasarlanabilecek iki tip bağlamsal terim vardır. Birinci tip terim, sınıfların (kavramlar) adlarıdır. Sınıflar veya grupların sınıflandırılması, varlıkların gruplar halinde kategorizasyonu kavramıdır. Sınıflar - insanlar, hastane, hastalıklar, bulgular, tanılar, oteller, yazarlar ve kitapları olabilir. Basitçe söylemek gerekirse, hakkında yorum yapılabilen nesne veya varlıklardır. Örneğin, adı, kimlik numarası, mesleği gibi tanımlardan oluşan bireyi, kişi sınıfı olarak tanımlayabiliriz. Bir de her sınıf için alt sınıf - üst sınıf ilişkileri olabilir. Bu anlamda bir "Kişi" sınıfı, hastane, üniversite gibi bir kurumdaki rolleri kategorize eden alt sınıflara sahip olabilir. Diğer bağlamsal terim tipi ise iki sınıfı bir arada ilişkilendiren isim özelliğidir. Aynı zamanda özellikleri, yüklem olarak ele alınabilir. Yüklem, bir takım özelliklere göre daha genel ilişkileri içerir ve iki varlık arasındaki herhangi bir ikili ilişkiye değinir. Aslında, sınıflar arasındaki bir ilişki, iki varlık arasındaki bağlantı olarak yorumlanabilir. Bu çerçevede, bağlamsal terimlerin her ikisi de OWL kullanılarak temsil edilebilir.



Şekil 4.5 Ontoloji Bağlam Modeli

Şekil 4.5'te varlık tabanlı bağlam modeli için bir üst seviye ontoloji modeli OWL dili kullanılarak oluşturulmuştur. Bu model, "bağlam varlıkları" ve "bağlam bilgileri" olmak üzeri iki ana sınıf üst ontolojisinden oluşmaktadır. Bu çerçevede, modelde yer alan üst sınıf - alt sınıf ile bağlam varlıkları arasındaki

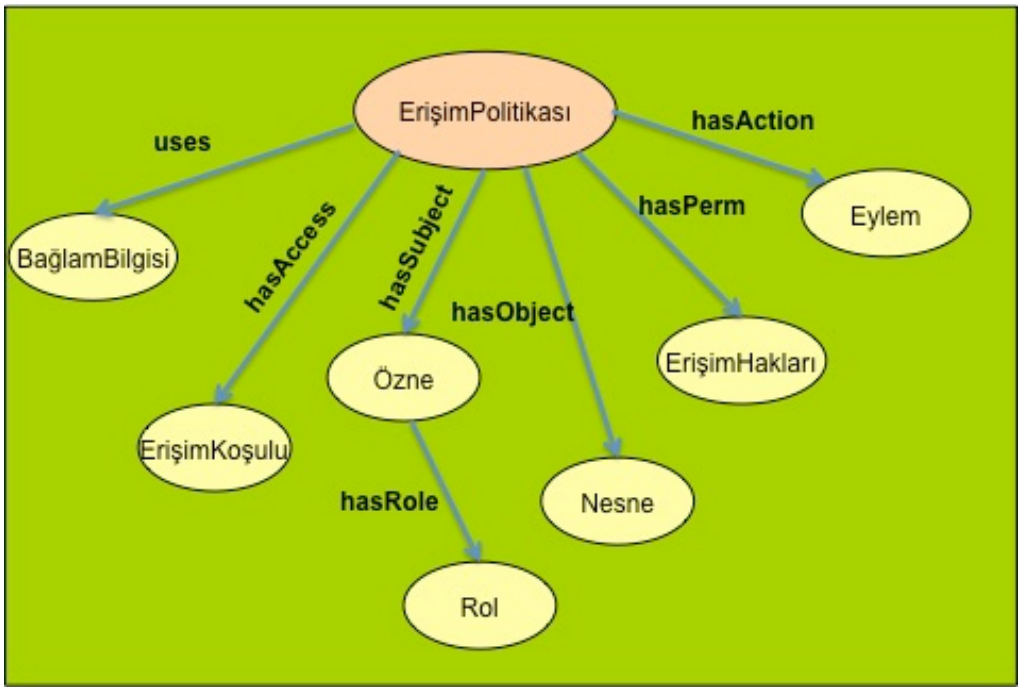
ilişkisinde “is-a” kullanılarak ifade edilmektedir. Bağlam varlıkları (sınıflar) hiyerarşik olarak düzenlenmiştir. Bu hiyerarşik yapı içinde “Kullanıcı”, “Kaynak”, “Kaynak Sahibi” ve “Çevre” gibi önemli bağlam varlıkları içermektedir. Bu anlamda “bağlam varlıkları” çekirdek ve çevresel olmak üzeri iki gruba sınıflandırılabilir. Burada “Kullanıcı”, “Kaynak” ve “Kaynak Sahibi” varlıkları bir erişim denetimi yaklaşımının temeli olan çekirdek varlıklardır. Aynı zamanda kullanıcı rolleri üzerinde erişim haklarını düzenleyen RBAC rol yaklaşımı uyarlanmasını sağlayacak “Rol” üst varlık sınıfı kullanılmaktadır. Bir kullanıcının bir rolü olduğunu tanımı için “Kullanıcı” ve “Rol” sınıfları arasındaki “hasRole” yüklem ilişkisine sahiptir. Bu çerçevede, dinamik rollerin atanması işlemleri gerçekleştirilmesini sağlayacak “Kimlik” üst varlık sınıfı kullanılmaktadır. Aynı şekilde, “Kullanıcı” ve “Kimlik” sınıfları arasındaki “hasCredential” yüklem ilişkisi söz konusudur. Kullanıcı ve Kaynak arasında ise “has” yüklem ilişkisi mevcuttur. Aynı şekilde “Kaynak” ve “Sahibi” sınıfları arasında “isOwn” ilişkisi söz konusudur. Çevresel varlıklar ise erişim isteği ile ilgili diğer varlıklardır.

4.2.3 Politika Modeli

Erişim denetim politikaları, belirli uygun koşullar altında bir öznenin uygun koşullar nesne varlığını üzerinde belli bir eylem/eylemleri gerçekleştirmesi için erişim izni veya reddi belirtir. Politika genelde, “İzin” ve “Reddet” kararları döndüren kural bileşenlerinden oluşan kısıtlama kurallar biçiminde yazılır. Her bir politika, etki alan bilgisi ile ilişkilendirilmelidir. Ayrıca, politika değerlendirme işlemini kolaylaştırmak için her öznenin korunan kaynak üzerinde sahip olduğu hakları durumuna göre yetkilendirmeyi uygulanır. Bağlama dayalı erişim kontrolünde, erişim denetimi gerçekleştirmek için bir politika durum bağlamları kullanması gerekir. Bu nedenle, semantik bağlamları elde etmek için alan bilgisi üzerinden sonuca varılması gerekir. Başka bir deyişle, tutarlı bağlam bilgileri elde etmek için söz edilen kurallar, bilgi tabanı üzerinde sonuç parametreleri sahip olmalıdır.

Bağlama-dayalı erişim kontrol politikası, bağlam ontolojisinden anlamsal bağlamları elde etmeye çalışır. Bu çerçevede, “Erişim Politikası”, “Özne”, “Rol”, “Nesne”, “Erişim Hakları”, “Eylem” ve çevre koşulları yaklaşımları içeren bağlama-dayalı politika ontolojisi Şekil 4.6’da gösterilmiştir. Buna göre erişim

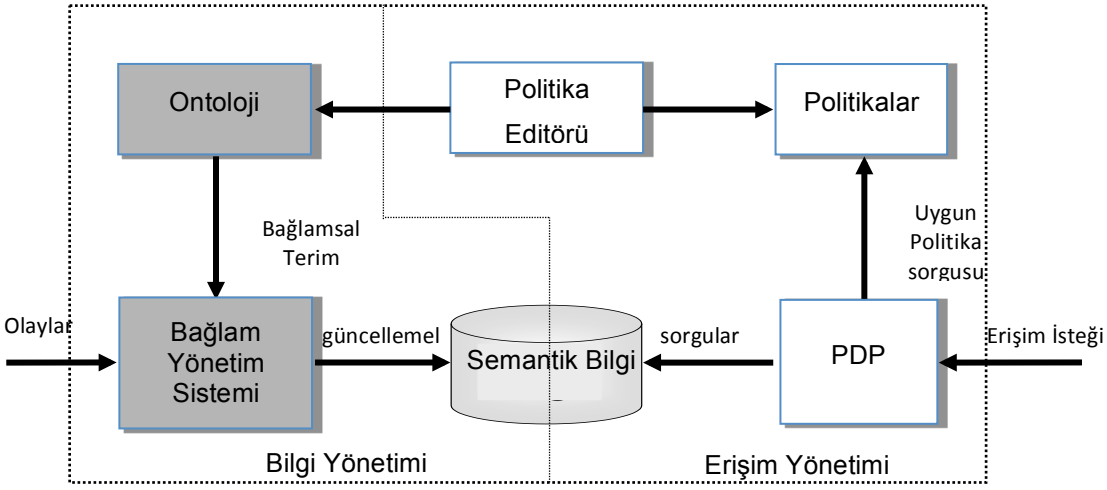
politikası, bir öznenin (bir role sahip olan) belirli bir nesne (öncelikli düzeyine göre) üzerinde bağlama dayalı erişim koşulları altında belli bir eylemleri (okuma veya yazma) gerçekleştirmesi için erişim izni olup olmadığını belirler.



Şekil 4.6 Bağlama-Dayalı Politika Ontolojisi

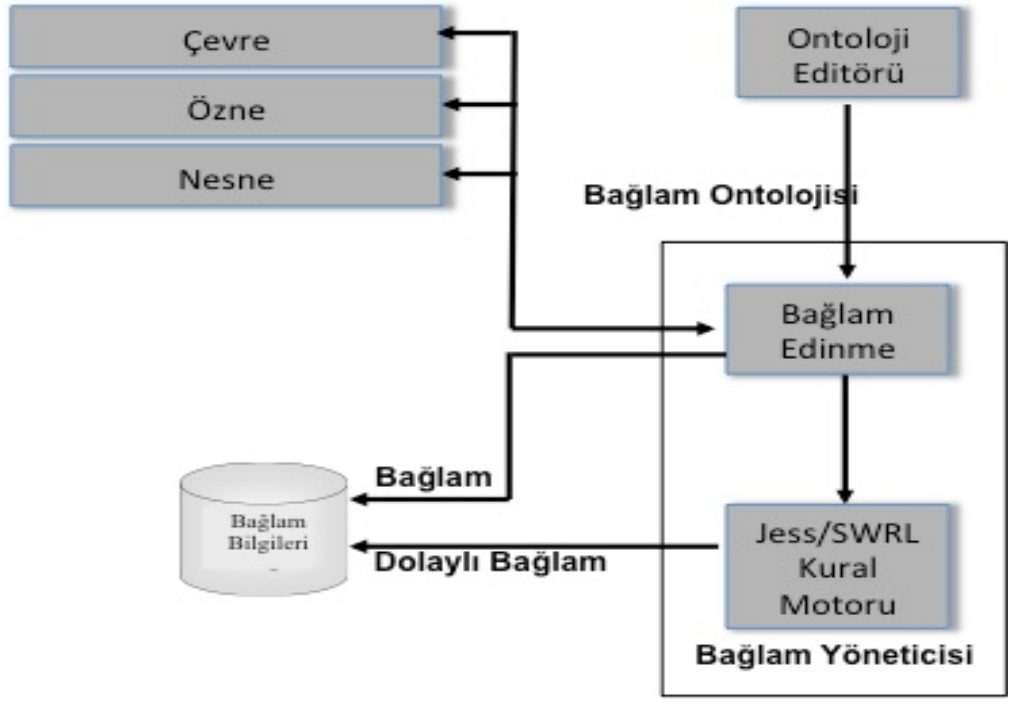
4.2.4 Kavramsal Çerçeve

Bağlama dayalı erişim denetim modelleri denildiği zaman, erişim yönetimi ve bağlam bilgi yönetimi gibi iki parçadan oluşan kavramsal çerçeveden söz edilir (Şekil 4.7).



Şekil 4.7 Kavramsal Çerçeve [62]

Bilgi yönetimi için belirli bir alanın terimlerini ve sınıflandırmalarını kapsayan ontolojik çerçeveler gerektirmektedir. Bu kapsamda bağlam yönetim sistemi, etki alan eylemler üzerinde anlamsal bilgi tabanı güncellemelerini ya da gerekli değişikleri gerçekleştirir(Şekil 4.8). Erişim yönetimi ise erişim denetim politikalarının oluşturulması için gereken bir politika editörü olarak düşünebilir. Politika editörü, politikalarda kullanmak üzere etki alan sözlüklerinden oluşan ontolojiye erişme yeteneğine sahip olmalıdır. Başka bir deyişle, politika editörü – etki alanı ontolojisine bakılarak uygun bağlamların sıralama yeteneğine sahip olması gerekir. Bu çerçevede, bir politika sisteminin gelen erişim isteği mesajına müdahale ederek, söz konusu istek iletisi için uygulanabilir uygun bir politikayı araştırır. Bu süreçte politika sistemi, o politikanın gerektirdiği ilişkileri(bağlamları) bulabilmek için anlamsal bilgi sorgu iletisinde bulunur. İşlemin sonucunda politika sistem tarafından izin onayı ve reddi iletisi bildirilir.



Şekil 4.8 Bağlam Yönetim Sistemi

Bu yapıdaki bir politika sistemi, bağlamlarda semantik çerçeveyi anlayabildiği sürece varlıklar ve bağlamlar arasında tüm olası örneklemleri manuel yazmaya gerek kalmamaktadır. Ayrıca sadece bağlam bilgileri temelinde politika tanımlamayla kısıtlı kalmayıp, mevcut bağlamla ilişkili olarak politikaların sorunsuz adaptasyonunu sağlayan politika belirleme yeni bir yaklaşıma gerek duyulmaktadır.

Bu çerçevede, bir politika tanımıyla dilin aranan nitelikleri söyle sırlayabiliriz:

- İyi tanımlanmış semantik: Tanımlanacak anlamlı politikalar uygulamadan bağımsız ve tutarlı olmalı;
- Değerlendirme tipi: burada üç değerlendirme tipi söz konusudur: merkezi - tüm bilgileri yerel olarak bulunduran, dağıtık politikalar – politikalar dağıtık olmasına rağmen karar düzeneğinin merkezi olarak gerçekleştiren ve dağıtık değerlendirme – politikalar ve karar süreçleri dağıtık şekilde olan.
- Değişkenler kullanımı: semantiği genişletebilme, farklı kuralların birleştirilmesi, yüklemlerin güncellenmesi;
- İşlemler/Birleşimler: ayırtım, birleşme, NOR, XOR v.s. işlemleri uyarlanabilmeli;
- Kural tabanlı: birçok politikaları, olay, koşul ve eylemleri kurallar dizini şekilde tanımlayabilme veri yapısına sahip olmalı;
- Genişleyebilir: Bir politika dili, yeni ihtiyaç duyulan kavramsal koşulları kapsayacak şekilde uyarlanabilir olmalıdır;
- Kullanışlı: özel politika dili uzmanlığı gerektirmeden kullanılabilecek ve anlaşılır bir yapıya sahip olmalı;

4.3 Genişletilebilir Erişim Kontrolü İşaretleme Dili (XACML)

Yetkilendirme, kullanıcıların kaynak erişimine izin veren ya da engelleyen ve bilgi güvenliğinin en önemli erişim denetim standartlarından biridir. Bu çerçevede, dağıtık bir ortamda kapsamlı ve bütünleşik (entegre) güvenlik çözümleri sağlamayı hedefleyen bir yetkilendirme işlemini gerçekleştirilebilmesi için XML tabanlı güvenlik politika dillerinin kullanımı söz konusudur. Aynı zamanda erişim denetimi alanında politikaları oluşturmak ve erişim denetimi kurallarını belirlemek amacıyla bir standart dil yapısına duyulan ihtiyaç doğrultusunda bir dizi çalışmalar yapılmıştır. Bu çalışmalardan geniş bir tanımlama yapısına sahip olan XACML (eXtensible Access Control Markup Language) dili kabul görmüş yaygın bir yaklaşım olarak karşımıza çıkmaktadır. Güvenlik standartları OASIS (Organization for the Advancement of Structured Informatıon Standards) [57] tarafından önerilen XACML, nesnelerin yetkilendirme politikalarının da XML biçiminde tanımlanması için tasarlanarak, çoğu politika gösterim düzeneklerinin işlevselliklerini de ifade edebilmektedir. XACML politika dilinin temel mantığı, herhangi bir rolden gelen kaynak erişimine olumlu veya olumsuz bir şekilde cevaben karar düzeneği işlevini görmesidir. XACML dilinin en önemli üstün özelliklerinden biri de dağıtık mimariyi de destekliyor olmasıdır. Bu anlamda dağıtık bir ortamda bulunan sistemleri kendine uygun olarak alt politikalar düzenler ve XACML hazırlanan bu farklı politikaları uyumlu bir biçimde yönetmeyi sağlar. Ayrıca farklı kuralları ve politikaları değişik durumlarda birleştirebilme ve erişim denetim üzerinde kaynak nesneyi koruma politikaları betimleme olanağı vermektedir. XACML dili, üzerinde yeni fonksiyonlar, veri tipleri, birleştirme algoritmaları tanımlanarak da genişletilebilir. Bu araştırma çalışması kapsamında XACML dili üzerinde durulmasının bir kaç nedeni vardır:

- Standart: XACML, yaygın olarak kabul gören standart bir erişim denetim dilidir. Yetkilendirme sistemi tasarlama aşamasında, yeni bir politika dili geliştirilmesi gerektirmiyor;
- Kapsamlı: XACML, herhangi bir özel uygulama veya kaynağa bağımlı değil. Web servis, firewall, kaynak yönetimi gibi çeşitli ortamlara

uygulanabilir. Farklı uygulama sistemlerinde kullanabilecek politikaların yazılmasına olanak sağlar;

- Dağıtık: Politikalar dağıtık bir yapıda olup, bir sistemden diğer sisteme aktarılabilir. XACML, politika birleştirme algoritmaları aracılığıyla farklı sistemlerden gelen politika sonuçlarını birleştirme yeteneğine sahiptir;
- Genişletilebilir: XACML, farklı veri tipleri, fonksiyonlar ve kuralları birleştirme algoritmalarını desteklemektedir. Bu dili, üzerinde yeni fonksiyonlar, veri tipleri, birleştirme algoritma tanımlayarak da genişletilebilir. Buna ek olarak da, RBAC ve SAML (Security Assertion Markup Language) profilleri için standart uzantı ve profilleri mevcuttur.

XACML politikalarının, bu politikaları belirleyenin politikaları hazırlamak için bilmesi gereken birçok kuralın olması ve politikalarda çok fazla kavramın yer almasının politikaların karmaşıklaşmasına yol açması gibi eksikleri vardır. Bu eksikliklere rağmen XACML erişim denetimi için iyi bir alternatiftir. Esnek ve iyi şekilde tasarlanmış olan XACML standardı, bahsi geçen eksiklikleri telafi edebilir.

XACML mimarisinin yapısına bakıldığında, dört önemli bileşenin mevcut olduğu görülmektedir:

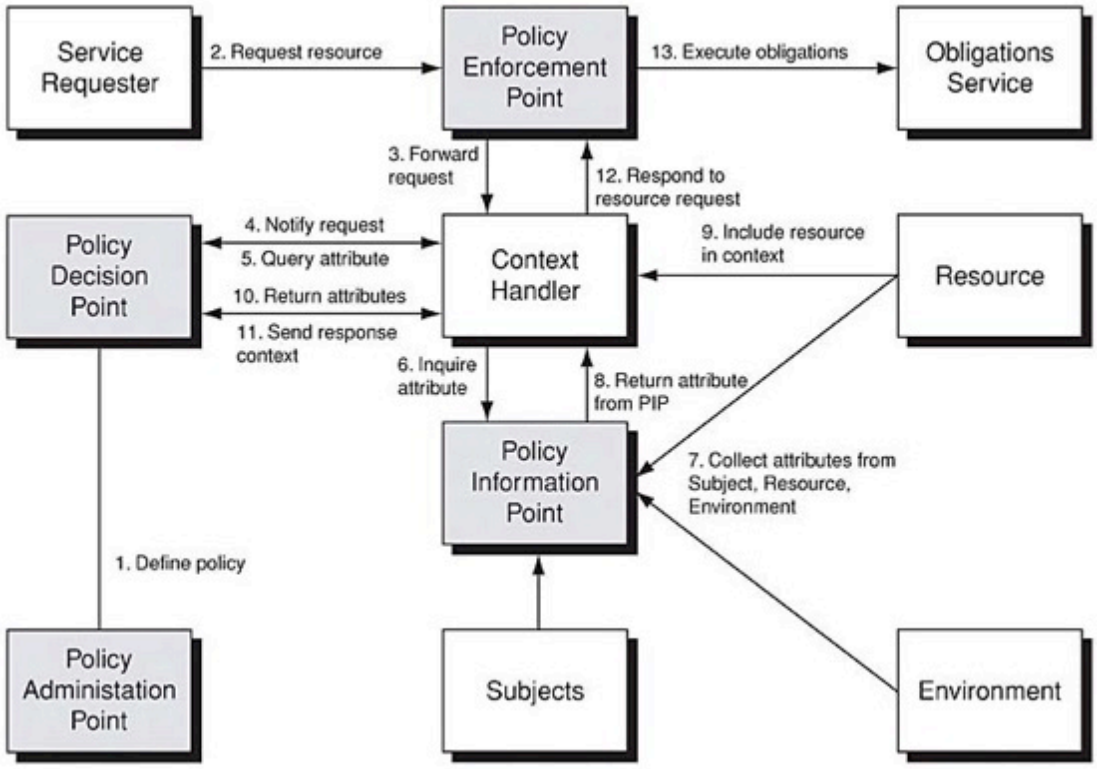
- Politika Yürütme Noktası (PEP) – Politika uygulama işleminin gerçekleştirildiği merkezdir. Kullanıcı veya servisten gelen talebi XACML isteğine dönüştürerek, PDP tarafından gelen yanıt kararın yorumlama işlemini gerçekleştirir;
- Politika Karar Noktası (PDP) – Politika karar sonuç merkezidir. PEP'ten gelen XACML biçimindeki isteği alır ve bu isteğin PAP üzerindeki politikalara göre yetkisinin olup olmadığına karar verir ve sonuç kararı PEP'e iletir;
- Politika Yönetim Noktası (PAP) – Politikaların yönetiminin yapıldığı merkezdir. Gerekli güvenlik politikalarını oluşturur ve uygun biçimde depolar;
- Politika Bilgi Noktası (PIP) – Politikalara bilgi sağlayan merkezdir. Politikalarla ilgili bilgilerin ve özelliklerin yer aldığı yerdir. PDP karar verme işlemi için gerekli bilgiyi sağlayan bileşendir;

XACML üzerinde birden çok politika mevcuttur. Bu anlamda, her bir politikaya göre gelen istekler politikalar tarafından değerlendirme işlemini yerine getirir ve yanıt bilgileri oluşturulur. Oluşan bu yanıt bilgiler, politika birleştirme algoritması temelinde izin, reddetmek ve uygulanamaz biçiminde tek bir sonuç yanıtı oluşturulur.

XACML çalışma mekanizmasının temel olarak, politikaları birleştiren algoritmalardan oluştuğu söylenebilir. XACML belirtimleri veri akışı modeli ve dil modeli sağlamaktadır.

4.3.1 Veri Akış Modeli

XACML veri akış modeli, modelin varlıkları arasındaki iletişim protokollerini belirtmez (Şekil 4.9). Böylece bu işlem geliştiricinin kararına kalmıştır. Bu modelin işleyiş şekli aşağıda sıralanmıştır [57]:



Şekil 4.9 XACML Veri Akış Diyagramı [57]

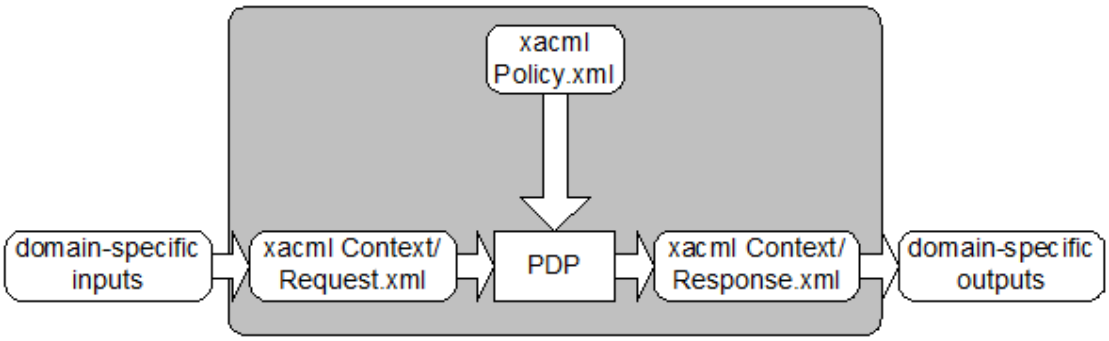
1. PAP – politikalar ve politika kümeleri oluşturur ve PDP tarafından kullanabilir biçime getirir. Bu politikalar veya politika kümeleri, tamamlanmış politikayı temsil eder.

2. Talepte bulunan varlık tarafından PEP'ye erişim isteği gönderir;
3. PEP aldığı erişim isteğini bağlam işleyicisine gönderir. Burada ek seçenek olarak, istek biçiminde özneler, nesneler, eylem ve çevre öznitelikleri bilgileri de yer alabilir;
4. Bağlam işleyici XACML istek bağlamı oluşturur ve politika değerlendirme işlemi için PDP noktasına gönderir;
5. PDP tarafından özne, kaynak, eylem ve çevre ile ilişkin bağlam işleyiciden herhangi bir ek bilgi isteği alabilir;
6. Bağlam işleyici, özellikleri ilgili bilginin (özneler, kaynaklar, servisler vb) PIP tarafından gönderilmesi isteğinde bulunur;
7. PIP ihtiyaç duyulan özellikler ilgili bilgiyi alır;
8. PIP söz konusu bilgiyi bağlam işleyicisine gönderir;
9. Ek olarak, bağlam işleyicisi bağlamda kaynak bilgisini içerir;
10. Bağlam işleyicisi elde ettiği özellikleri ve kaynak (seçmeli) bilgilerini PDP'ye gönderir. PDP ise politika değerlendirme evrim işlemini gerçekleştirir;
11. PDP, bağlam işleyici için bağlam yanıt (yetkilendirme sonuç kararı dahil olmak üzeri) sonucunu döndürür;
12. Bağlam işleyici aldığı bağlam yanıt bilgisini PEP için uygun biçime çevirir ve PEP bu bilgiyi döndürür;
13. PEP yükümlüklerini yerine getirir;
14. Eğer erişim izni verildiyse, PEP ilgili kaynağa erişim izni verir. Aksi durumda, erişim engellenir.

4.3.2 XACML Bağlamı

XACML, geniş çaptaki çeşitli uygulamalarda rahatça kullanılabilecek şekilde tasarlanmıştır. Böylece, "XACML bağlam" (Şekil 4.10) yaklaşımıyla çekirdek dili uygulama ortamından yalıtılmıştır. XACML bağlamı, sadece PDP'nin girdi ve çıktılarını temsil eder ve temelde özne, kaynak, eylem veya ek olarak çevresel ortam nitelikleriyle ilgilenir[58-34]. XACML dili, "xacml context" ve "xacml policy" olmak üzeri iki XML şemaları ile tanımlanır:

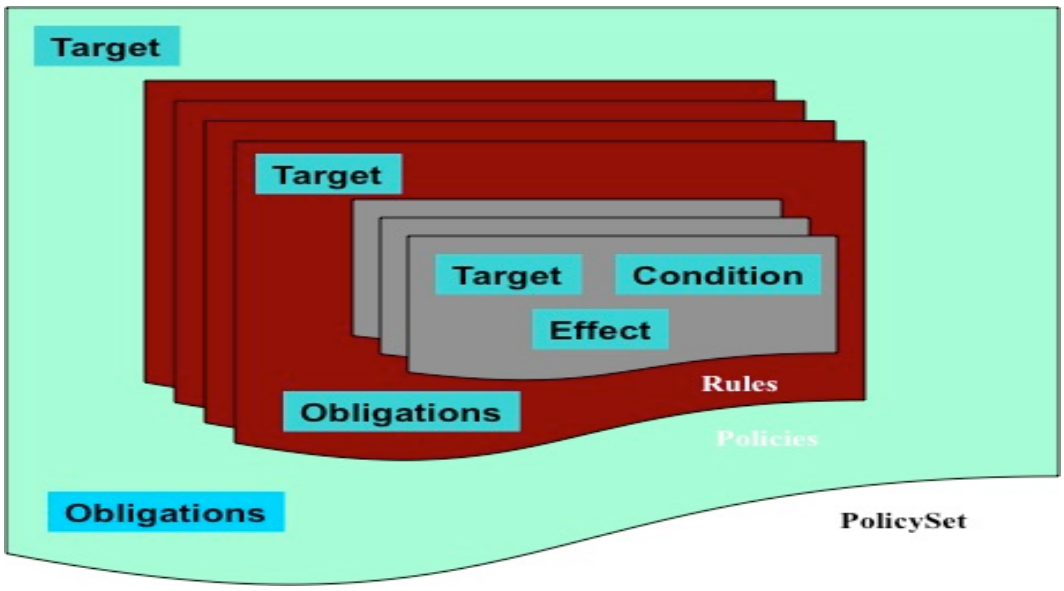
- “xacml context”, PEP ve PDP arasındaki politika isteği ve politika geri bildirim iletilerin değiştokuş işlemlerin nasıl temsil ettiğini belirler;
- “xacml policy”, erişim denetim politikaların nasıl temsil ettiğini belirler;



Şekil 4.10 XACML Bağlamı [57]

4.3.3 XACML Politika Dili Modeli

XACML politika dili modeli temel olarak “Kural”, “Politika” ve “Politika kümesi” kavramlarından oluşmaktadır. “Politika Kümesi”, diğer politika ve politika kümeleri tanımlamalarını tutan bir küme veya dağıtık sistemlere bulunan politikalara olan referansları da tutmaktadır.



Şekil 4.11 XACML Dil Modelinin Grafiksel Görünümü [57]

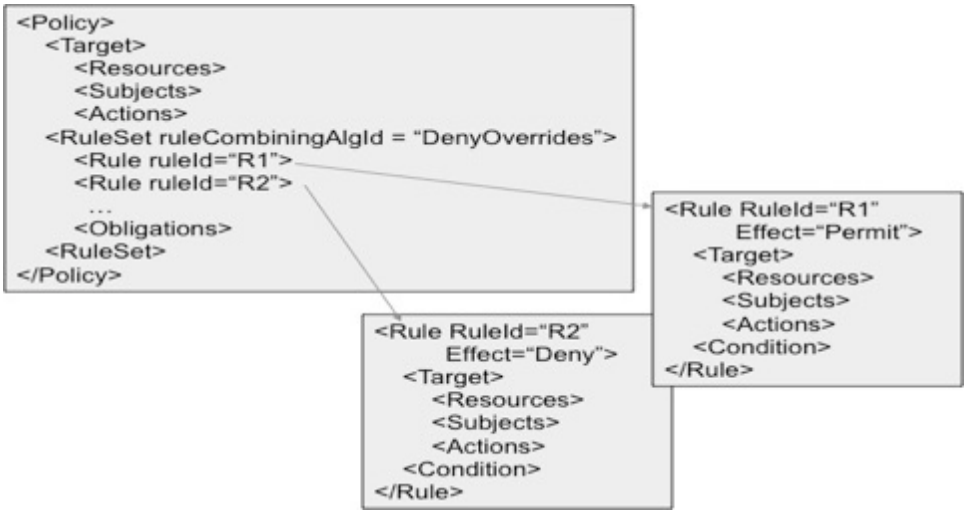
Aynı zamanda “Politika”, kurallar kümesi ile ifade edilen yalnızca bir erişim denetim politikasını temsil etmektedir. Kural ise bir politikanın temel bir

birimidir. Her bir XACML politika belgesi sadece ve sadece bir “Politika” veya “Politika Kümesi” kök XML etiket elemanlarını içermektedir. Ayrıca bir “Politika” veya “Politika Kümesi”, birden fazla politika ve her biri farklı erişim denetim kararlarını etkileyebilecek kurallardan oluşmaktadır. Şekil 4.11’da XACML dil modelinin grafiksel görünümü verilmiştir.

Burada “*Rule*” olarak tanımlanan kurallar, XACML’in karar verme aşamasındaki en temel elemanıdır. Bu anlamda “*Rule*”, erişim isteğini girdi olarak alan ve erişimle ilgili izin verip verilmemesine karar veren bir fonksiyondur. Birçok kural durum koşulları setinden oluştuğundan, oldukça karmaşık olabilir.

XACML, her çıkan kararı uzlaştırma düzeneği gerektirmektedir. Bu ise birleştirme algoritmaları toplamı ile gerçekleştirilmektedir. Burada politika birleştirme algoritmaları (politika kümesi tarafınca kullanılır) ve kural birleştirme algoritmaları (politika tarafından kullanılır) söz konusudur. Birleştirme algoritmaları, giderek karmaşık hale gelen politikaların kurulması için kullanılır. Gerektiğinde bu çeşitli standart algoritmalar dışında, başka yeni algoritmaları geliştirerek genişletilme olanağı da mevcuttur.

PDP görevlerinden biri de, belirli bir istek için geçerli politikaları bulmaktır. Bunu yapabilmek için, XACML “*Target*” isimli özelliği (etiket) ile sağlamaktadır. Eğer bir kural, bir erişim isteğine uygulanabilecek ise, “*Target*“ elemanı kullanılır. “Target” etiketi, verilen bir talebe uygulanabilmek amacıyla bir kurala uyan özne(*Subject*), kaynak(*Resource*) ve eylem(*Action*) tanımlamaları için kullanılan basitleştirilmiş koşullar setidir. *Target* etiketle gelen bir talep içindeki değerleri karşılaştırma işlemi için mantıksal işlevleri kullanmaktadır. *Target* etiketindeki tüm koşullar karşılaştırılarak, uygulanabilirliğini denetlemektedir. Bunun dışında birçok politikaların depolandığı bir ortamda geçerli olan politikayı bulma işlemini hızlıca gerçekleştirebilmek için *Target* bilgisinde politikaları indekslemesi sağlanmaktadır. Şekil 4.12’da XACML dil modelinin XML görünümü verilmiştir.

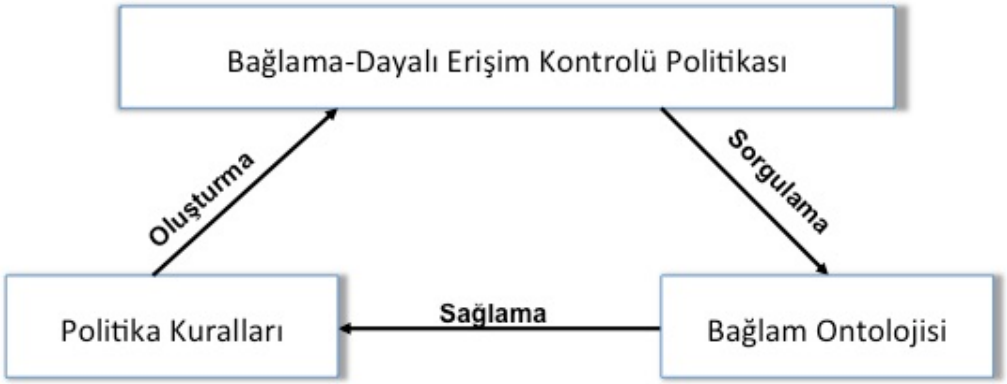


Şekil 4.12 XACM Dil Modelinin XML görünümü [57]

4.4 Anlamsal Bağlama-Dayalı Erişim Kontrol Politikası

Genelde politikalar, "Reddetmek" veya "İzin" sonuç kararı döndüren kısıtlı kurallar biçiminde yazılmaktadır. Her politika alan bilgisi ile ilişkilendirilmiş olması gerektirir. Bağlama dayalı sistemde, bir politikanın anlaşılır olması gerekir ve erişim denetimini gerçekleştirmek için durumsal bağlamları kullanmalıdır. Bu nedenle, bağlamlarda semantik bir çerçeve elde etmek için etki alan bilgisi üzerinde sonuca varılması gerekmektedir. Şekil 4.13'de bir bağlama dayalı erişim politikası, politika kuralları ve bağlam ontolojisi (semantik bağlam) arasındaki ilişkileri göstermektedir. Politika kuralları erişim izni verebilmek için durumsal veya tanımlanmış bağlamlara ihtiyaç olabilir ya da olmayabilir. Bağlam ontolojisi, ilgili bağlamları sağlar ve anlamsal politika için politika kuralları oluşturur. Bağlama-dayalı erişim denetim politikası, bağlam ontolojisinde elde edilen bağlamların anlamlarını yorumlama işlemini gerçekleştirir. Semantik bağlamların erişim denetim politikasına kolayca entegrasyonu yaklaşımlarından biri de, her bağlam erişim denetim politikasında anlaşılacak kuralların eklenmesidir. Bu ise çok zor bir süreçtir.

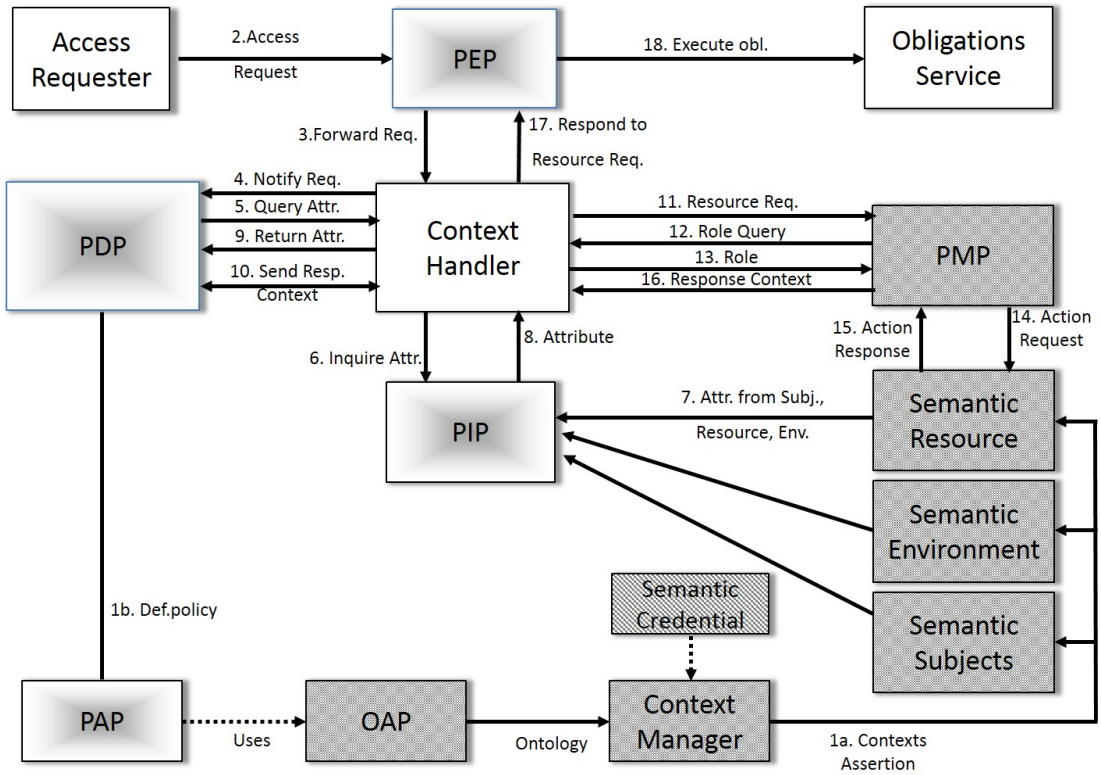
Bunun çözümü olarak da, politika üzerinde söz konusu kuralları gömmeden semantik bağlamların erişim denetim politikalarında doğrudan kullanılabilmesini sağlayacak, XACML üzerinde ek değişiklikler temelinde genişletme yaklaşımın gerçekleştirilmesidir.



Şekil 4.13 Bağlama-Dayalı Erişim Kontrolü Politikası Oluşturma Süreci

4.4.1 XACML'in Genişletilmesi

XACML'ın RBAC profili ile erişim denetim politikalarıda rol kavramını ifade edebilmektedir. Ancak rolün sahip olduğu yetkileri başka bir role devir etme düzeneklerinin uygulanma işlemleri XACML'ın standart RBAC profilide yönetilmesi çok karmaşıktır. Erişim denetim politikalarını iyi bir şekilde ifade edebilen yeni XACML profili ile birlikte erişim kuralların kolayca güncellenmesi ve manipüle eden esnek modeli uyarlanması gerekmektedir.



Şekil 4.14 Genişletilmiş XACML Veri Akış Diyagramı

Yetkilendirme işlemi içinde her özne ve kaynağın birden fazla nitelik değerlerini içerebilme avantajı sağlayan XACML özelliğini kullanarak, semantik bağlamların erişim denetim politikasına entegrasyonu söz konusudur.

Özne veya kaynağa özgün niteliklere temelinde bir erişim denetim karar değerlendirmesi gerçekleştirilebilir. Başka bir deyişle, özne veya kaynak niteliklerine dayanılarak politika oluşturulabilir. Bu anlamında, semantik bağlamları < AttributeID > etiket değerleri olarak politikaya entegre edilebilir. Bu yaklaşım bir erişim isteği üzerine sadece özne ve kaynak nitelikleri için uygulanmaktadır. Aynı zamanda semantik bağlamların, nitelik değerleri olarak da entegre edilmesi mümkündür. PEP bileşeninden gelen bir erişim talebi üzerine özne ve kaynak ile birlikte bağlamların da ilişkilendirilmesi çok önemlidir. Bu yaklaşımın en önemli noktası, özne ve kaynak ile birlikte ilişkilendirilen bağlamları bulmak için semantik bilgi tabanı üzerinde sorgu düzeneğinin kullanılmasıdır. Şekil 4.14'de genişletilmiş XACML sisteminin veri akış diyagramı sunulmuştur. Bu tezde önerilen yaklaşım, genişletilmiş XACML veri akış diyagramına koyu renkle belirtilmiş eklentiler yapılarak elde edilmiştir. Buna göre, bağlama dayalı bir erişim kontrol karar değerlendirme ve yürütme süreci aşağıda belirtilen süreçlerden geçmektedir:

1. a. Bu adım, bir ön işlem aşamasıdır. Bu aşama, Ontoloji Yönetim merkezinde (OAP) bir bağlam ontolojisi oluşturularak başlar. Ontoloji, bağlam yöneticinden yüklenir;

   b. PDP bileşeninde kullanılması için XACML politikası PAP tarafından oluşturulur. Burada PAP - normal XACML işlem sürecinden farklı olarak, bağlam ifadeleri ve bağlama dayalı erişim denetim biçimini kullanabilmek amacıyla OAP üzerindeki ontolojiyi göz önünde bulundurur;

2. Talepte bulunan özne varlığı tarafından kaynağa erişim isteğini PEP'ye iletir;

3. PEP aldığı erişim istek iletisini bağlam işleyiciye gönderir. Burada ek seçenek olarak, istek biçiminde özneler, nesneler, eylem, kimlik tanıma ve çevre nitelikleri bilgileri yer alabilir;

4. Bağlam işleyici XACML istek bağlamı oluşturur ve politika karar değerlendirme işlemi için PDP noktasına gönderir;
5. PDP tarafından kimlik tanıma, özne, kaynak, eylem ve çevre ile ilişkin ek bilgiyi içeren iletiyi bağlam işleyiciden alır;
6. Bağlam işleyici, bu ek nitelikler ilgili bilginin (kimlik tanıma, özneler, kaynaklar, servisler vb) PIP tarafından gönderilmesi isteğinde bulunur;
7. PIP ihtiyaç duyulan, durumsal bağlamları içerebilen semantik kimlik tanıma, özne, kaynak ve çevresel ortam nitelikli bilgiyi alır;
8. PIP söz konusu nitelikli bilgiyi bağlam işleyicisine bildirir;
9. Bağlam işleyicisi elde ettiği nitelikli bilgileri (bağlam nitelikleri dahil) ve kaynak (seçmeli) bilgilerini PDP'ye gönderir;
10. PDP, bağlam işleyicisinden gelen kimlik bilgileri dahil olmak üzeri bağlamsal niteliklerine uygun rolü kullanıcıya atama işlemini gerçekleştirir ve bağlam yanıt sonucu döndürür;
11. Bağlam işleyici aldığı bağlam yanıt bilgiyi, yetki yönetim noktasına (PMP) bildirir;
12. PMP, rol sorgusunu bağlam işleyicisine geri bildirir;
13. Bağlam işleyici, istenilen rol nitelik bilgileri (PDP tarafından rol atama bilgileri) içeren PMP noktasına yanıt bilgisini gönderir;
14. PMP, gelen bağlam isteğine uygun kaynağı eşleştirme işlemi gerçekleştirir ve istek mesajını oluşturur;
15. PMP, rollere göre politka ve eylem izinleri birlikte değerlendirme işlemi gerçekleştirir ve bağlam işleyiciye yanıt bağlam bilgileri (yetkilendirme sonuç kararı dahil olmak üzeri) geri gönderir;
16. Bağlam işleyici aldığı bağlam yanıt bilgiyi PEP için uygun biçimine çevirir ve PEP bu bilgiyi döndürür;
17. PEP yükümlüklerini yerine getirir;
18. Eğer erişim izni verildiyse, PEP ilgili kaynağa erişim izni verir. Aksi durumda, erişim engellenir.

4.5 Çalışma ve Tartışma

Çeşitli araştırmalar, dağıtık ortamlarda veri paylaşılmasıda bilgiye yetkisiz erişimi denetleyen erişim kontrolü için genişletilmiş RBAC yaklaşımı uyarlama çalışmalarına odaklanmıştır. Dağıtık bilgi sistemlerinin geliştirme sürecinde, kullanıcılara rol ve yetki izni atama işlemleri çok karmaşık ve bağlamsal bilgilerl bağlı olmaya başladı. Bazı çalışmalarda, mekân ve zaman gibi belirli bağlam tipleri kullanılarak, erişim denetim düzenekleri geliştirilmeye çalışılmıştır. Bu çerçevede, kullanıcı ve kaynak niteliklerini bağlam kısıtları olarak kullanan bağlama-dayalı RBAC modeli Kulkarni [58] tarafından önerilmiştir. Hong [70] tarafından ise kullanıcı, kaynak ve çevre konseptleri üzerinde rol tabanlı bağlama-dayalı erişim kontrolü politika modeli geliştirilmiştir. Genelde bu yaklaşımlar, dinamik ortamları için yeterli olmayan bağlam tipleri kullanılmaktadır.

Bu tez çerçevesinde, genel bağlam modellemesine ek olarak, “kaynak sahibi” ve farklı kullanıcı özneler arasındaki ilişkisel kavramlarını içeren genişletilebilir ontoloji tabanlı bağlam modeli kurgulanmıştır.

Bu anlamda, Toninelli [59], bağlam üzerinde (kaynak erişebilirliği, kullanıcı rolleri, mekân ve zaman gibi) kaynak erişim izni sağlayan, ayrıca bağlam ve politika modelleri kapsayan ontoloji tabanlı kavramsal çerçeve üzerinde anlamsal bağlama-dayalı erişim kontrolü yaklaşımı önermiştir. Söz edilen yaklaşımlar birbirine benzer olmasına rağmen, “kaynak sahibi, kullanıcı ve kaynak sahibi arasındaki ilişki”, türetilen varlık durumsal bilgileri gibi günümüzün dinamik ortamıdaki erişim denetimi için önemli olan bir takım kavramlar bu modellerde ön görülmemiştir.

Bu tez çalışmasında kurgulanan yaklaşımda - sözü geçen kavramlara ek olarak, farklı kimlik güven düzeyine göre kullanıcıların hiyerarşi yapıdaki kaynak bilgilerine erişimi denetlenmektedir.

Bu çerçevede yapılan diğer çalışmalarda, bağlama duyarlı uygulamalar için erişim denetimi sağlayan genişletilmiş ABAC yaklaşımı üzerine yönelmiştir. Hulsebosch [60] kullanıcı konumu ve erişim tarihçesi temelinde bağlama duyarlı erişim kontrol çerçeveyi önermiştir. Corradi [61] tarafından, “kullanıcı konumu, kullanıcı eylemi, kullanıcı aygıtı, zaman, kaynak erişebilirliği ve

durumu” gibi bağlamları doğrudan ilişkilendirilerek erişim izinleri düzenleyen bağlama duyarlı erişim kontrolü modeli sunulmuştur. Bu yaklaşımlar, sınırlı bağlam kümeleri kullanılması gibi sınırlanması mevcut. Bu ise sağlık hizmeti alanı için önemli öncelikleri olan kullanıcının durumsal konumunu tutarlı belirlenmesi açısından yetersizdir.

Bu tez çalışmasında, “kullanıcı, kaynak, kaynak sahibi, çevre ve durumsal” bağlam varlıkları ve “mekân, zaman, durum, ilişkisel ve kimlik” bağlam bilgileri anlamsal olarak ifade eden ontoloji tabanlı genişletilebilir bağlam modeli önerilmiştir. Çizelge 4.1’de mevcut modeler ile önerilen bağlam modeli arasında karşılaştırma tablosu verilmiştir. Bu karşılaştırma tablosunda görüldüğü gibi önerilen modelde diğer modellere göre daha geniş bağlam bilgileri anlamsal olarak temsil eden ontoloji tabanlı bağlam kullanılmaktadır. Durumsal değişimi tanımlama ve belirlemek için SWRL kuralları kullanımı söz konusudur. Burada, sağlık hizmetleri etki alanı ile ilgili bağlam ontolojileri işleme işlevleri sağlayan “Bağlam Yönetici”, gerçek zamanlı kullanıcı durumsal konumu ön plana çıkarmaktadır. Bu ontolojiler, sağlık hizmetleri uygulamalarının gizliliği ve güvenli politika yönetimi için genişletilebilmektedir. Başka bir deyişle, üst düzey bağlam yorumlama işlemi için çıkarım motorü üzerinde bağlam bilgileri içeren erişim denetim politika modeli sunulmuştur.

Aynı zamanda Toninelli [63] tarafından, dağıtık ortamda güvenli ortak çalışma için semantik bağlama-dayalı erişim kontrolü çerçeveyi önermiştir. Bu yaklaşımda, OWL tabanlı bağlam modeli üzerinde bağlama-dayalı politika modeli tasarlanarak, XACML kuralı içerisinde açıklama mantığı kullanan politika ifadeleri tanımlanmıştır.

Anlamsal politika dilleri kapsamında, Kagal [66] tarafından, herhangi bir semantik web dili kullanarak politika yazma olanağını sunan Rei politika dili önerilmiştir. Ayrıca N3 dili içerisine Rei uyarlanarak Rein politika çerçevesi oluşturulmuştur [67].

	Çevresel Bağlam	Kişisel Bağlam	Mekân-Zamansal Bağlam	Durumsal Bağlam	İlişkisel Bağlam	Kimlik Bağlam
RBAC	X	X	X	X	X	X
ABAC	O	O	O	X	X	X
Temporal-RBAC	X	X	O	X	X	X
Location-Aware RBAC	X	X	O	X	X	X
Generalized RBAC	X	O	O	X	X	X
DRBAC	X	O	X	X	X	X
OBAC	X	O	O	X	O	X
SBAC	X	O	X	X	X	X
SCA-RBAC	O	O	O	O	O	O

Çizelge 4.1 Bağlam Yönetimi Karşılaştırma Tablosu

Diğer semantik politika dili ise KAoS politika dilidir. KAoS politikaları OWL tabanlı olup, tutarlı politikaları denetimi için çıkarım işlemleride DL düzeneği kullanmaktadır. Naumenko [64] tarafından, mobil web hizmetleri için kullanan semantik tabanlı erişim kontrolü modeli geliştirilmştir. Bu model, OWL ve SWRL dillerin tüm özelliklerini devir alan güvenlik tabanlı yaklaşımları yorumlayabilen ve direk model-teorik semantik ile uyumludur. Moussa [65] tarafından ise semantk web için semantik tabanlı bağlama-dayalı erişim kontrolü tasarlanmıştır. Bu modelde, bağlamsal bilgileri ifade edebilmesinde bağlam ontolojisi kullanılarak, çıkarım motorü üzerinde çalıştırmaktadır.

Ayrıca Damiani [68] ise semantik dayalı sistemi oluşturmak içn genişletilmiş XACML politika dili kullanılmıştır. Buna benzer çalışma olarak T.Priebe [69], XACML niteliklerini kullanabilmek için genişletilmiş politika dili önermiştir. Bu yaklaşımda, erişim denetim karar verme noktasına semantik yorumlama motorü eklenmiştir. Buna göre, erişim yapılmadan önce semantik yorumlama işlemi gerçekleştirerek, erişim istek sürecinin işlenmesi için önemli ölçüde süreyi kısaltmaktadır.

	RBAC	ABAC	Bağlama Dayalı RBAC	SBAC	SCA-RBAC
Rol Tanımı	O	O	X	O	O
Rol-İzin Atama	O	X	O	O	O
En az Yetki ilkesi	O	O	O	O	O
Bilinmesi Gereken İlkesi	X	O	X	X	O
Rol Hiyerarşi	O	X	O	O	O
Esnek Yetki Atama	X	O	O	O	O
Durum Dayalı	X	X	O	X	O
İlişkisel Erişim Denetim	X	X	X	X	O
Semantik Bağlam	X	X	X	O	O
Çıkarım Yorumlama	X	X	X	O	O
Politika Dili	XML	XACML	XML	OWL-DL	E-XACML

Çizelge 4.2 Erişim Kontrol Politika Yönetim Karşılaştırma Tablosu

Dersingh [62], yaygın ortam için semantk politika kullanan bağlama-dayalı erişim kontrolü modeli tasarlanmıştır. Bu çalışmada bağlamların nasıl elde edildiği ve anlamsal olarak tanımlandığı gösterilerek, XACML'ın genişletmek süretiyle erişim denetim politika içeresine entegre edilmiştir.

S.Verma, S.Kumar [71] tarafından, RBAC ve ABAC modellerin ortak özellikleri kullanarak, hibrit semantik erişim kontrol modeli tasarlanmıştır. Bu modelde, dinamik rol atama ve rollere göre yetki izni belirleme gib iki aşamalı erişim denetim işlemi gerçekleştirmektedir.

Buna benzer olarak bu tez çalşımasında, RBAC ve ABAC modellerinde karşılaşan sorunları dikkate alınarak, daha uygun erişim kontrol modeli tasarlayabilmek için her iki modelin özelliklerini kullanan model kurgulanmıştır. Önerilen yaklaşımda, RBAC kullanıcı rolüne göre yetki izni atama ve ABAC modelin öznenin kimlik nitelikleri üzerinden belirli nitelikteki nesneye erişim

izni gerçekleştirme gibi dinamik yapıtları entegre edilmeye çalışılmıştır. Bunun için kimlik ontolojisi temelinde yeni bir nitelik eklenerek XACML mimarisi genişletilmiştir. Aynı zamanda semantik SWRL dili aracılığıyla erişim denetim modelinde bağlam ve politika anlamsal olarak ifade edilebildiği gösterilmiştir. Burada kimlik ontolojisi, erişim denetim ontolojisi ile birleşitirilerek kullanıcı kimliği temelinde rollerin belirlenmesi ve durumsal bağlamlarla rollerin sahip olabileceği yetki izinlerin dinamik değişimi sağlayacak semantik bağlama-dayalı erişim denetim düzeneği önerilmiştir. Tez çalışması kapsamında önerilen genişletilmiş modeli, diğer modelerle karşılaştırma tablosu Çizelge 4.2'de verilmişir. Bu karşılaştırma tabloda yetkilendirme konseptleri üzerinde anlamsal bağlam ve durum dayalı karar düzeneğinin uyarlanabilme yetenekleri, ayrıca kullanılan politika tanımlama dilleri temel alınarak, önerilen SCA-RBAC modelinin diğer yetkilendirme modellerine göre farkı gösterilmektedir.

Sonuçta, önerilen model ve sistem mimarisi, anlamsal bağlamlar üzerinde rol ve yetki atama işlemi gerçekleştirerek, kullanıcının durumsal konumunu ön plana çıkarmaktadır.

5. ÖNERİLEN MODELİN UYGULANMASI

Günümüzde, sağlık sistemleri, tıbbi bilgileri daha iyi yönetebilme, işleyebilme, depolayabilme ve güvenli olarak korunmasını sağlayabilmeyi temin edecek yeni akıllı teknolojilere uyarlanmasına doğru gitmektedir. Bu uyarlama sürecinin temelindeki ana hedef, tıbbi hizmetlerin kalitesini, sistemlerin verimliliğini arttırmak ve çeşitli bağlamlar üzerinden gerçek zamanlı bilgiye erişilebilirliği sağlamaktır.

Bilgi sistemleri olarak, açık sistemler haline gelmeye başlayan ve mobil kullanıcıya uyarlayabilen daha esnek olması hedeflenmektedir. Yeni medikal kayıtlar ve sağlık sistemi bilgileri, hasta kayıtlarının farklı etki alanlarındaki kullanıcıların erişiminin söz konusu olduğu medikal bilgilerin dağıtık ortam üzerinde ortak kullanımına ihtiyaç duymaktadır.

Farklı sistemlerden erişilebilen merkezi “Elektronik Sağlık Kayıtları” nın evrimi, korunan kayıt bilgilerinin yedeklenmesine, hasta bilgilerinin her zaman aktif ve güncel tutulmasına yardımcı olur. Aynı zamanda sağlık sistemlerinin akıllı teknolojileri ve mobil hizmetlerle entegrasyonuna doğru evrimsel gelişim süreci - geleneksel sağlık bilgi sistemlerinin, medikal bilgilere kullanıcıların her yerden ve her zaman kesintisiz erişebilirliğini sağlayan yaygın sağlık bilgi sistemlerine dönüştürülmesi gerektiğinin altını çizmiştir.

Medikal bilgilerin gizliliği ve hassasiyeti göz önünde bulundurulduğunda, sıkı güvenlik prosedürleri temelinde erişimi gündeme getirir ve çeşitli sağlık alt sistemlerinin (hastaneler, klinik laboratuvarlar, medikal birimler gibi) kendine özgü kaynak bilgilerin korunma ihtiyacı da göz ardı edilmemelidir. Dağıtık ortamda kaynak bilgilerin paylaşımı, bir kullanıcının rolüne veya pozisyonuna göre erişim haklarını düzenleme yeteneğine sahip RBAC modeli ile uyarlanan erişim izinlerinin yönetimini etkiler. Çeşitli tipteki çoklu ortam içeriğine sahip olan medikal kayıtlar genellikle, XML tabanlı temsil edilmektedir. Bilindiği gibi XML, dağıtık ortamda veri paylaşımı ve değişimini kolaylaştıran standart bir dil olarak kabul edilmektedir. XML ile sağlık kayıt bilgilerin içeriği ve yapısı basit bir metin halinde ifade edebilmektedir. Böyle hassas bilgilerin paylaşımı göz önüne alındığında, farklı etki alanlarının yetkileri üzerinde dağıtık kaynaklara erişimi durumunda erişim denetimi düzenekleri son derecede önem

kazanmaktadır. Bu çerçevede, erişim haklarını XML politikası biçimine dönüştüren XACML standart dilinin kullanımı söz konusudur. XACML, dağıtık erişim politikalarını yönetmek için tasarlanmış etkin karar verme düzeneğini sağlayan XML tabanlı standart bir dildir.

5.1 Sağlık Sistemlerinde Erişim Kontrolü Modeli

Medikal veriler, hassas, özel ve gizli bilgiler olarak kanunen kabul edilmektedir. Bu çerçevede medikal bilgilerin yüksek düzeyde korunması ve sıkı yönetilmesi gerekir. Sağlık sistemlerinde, bilgi erişimi yönetimi ve güvenlik kısıtlarının tanımlanma işlemi daha da zor bir hale almaktadır. Erişim denetimi, kaynak bilgilerine erişmek için bir isteğin sistem tarafından izin verilip verilmeyeceğini belirleyen bir düzenektir. Erişim denetim düzeneği, erişim hakların belirlenmesi sadece kullanıcı rolü veya pozisyonu temelinde olmayıp, mekân, zaman ve erişim isteğinin yapıldığı ortam gibi bağlamsal kısıtlar üzerinde gerçekleştirilmektedir

Bağlam, belli bir anda: yer-zaman-hizmet sunum noktası (acil servis, ameliyat masası), tanı süreçleri içerisinde bulunulan hizmet sunum noktaları (radyoloji, kontrast maddeyle yapılan tetkiklerin gerçekleştirildiği görüntüleme sistemleri vb…) durumu tanımlayıcı veri/bilgi setlerinin tümünün oluşturduğu ontolojik çerçevede oluşur.

Tıbbi pratikte, karşılaşılan durumu kayıt altına almak üzere çoğunluğu kodlama ağırlıklı (ICD 9, ICD 9-CM, ICD 10, ICD 10 CM, ENCODE FM, SNOMED CT, ATC…) sınıflandırma sistemleriyle, belli branşlar çerçevesinde uzmanlaşan tanımlayıcı setler belirginlik kazanmıştır ve bu eğilim devam etmektedir. Ancak, bu işin ve kalitesinin kesin çözümü ve belirleyicisi entegre edilebilen biyomedikal ontolojik çerçevelerdir.

Sebep-sonuç ilişkilerinin kurulabilmesine imkân sağlayacak semantik ve ontolojik yapılar henüz olgunlaşmamıştır. Bu olgunlaşmanın göstergeleri klinik kılavuzların tıbbi pratiğe girmesi, şikayet/semptomlar ve tanılar/tedavilerin bu alanda uygulama yazılımı geliştirmeye dahil olmasıdır. Olayın semantik içerik ve karar verme süreçlerine yeter düzeyde yansıması da ayrı bir olgunluk göstergesidir.

Özetlemek gerekirse, sağlanan teknik olanakları etkili ve verimli bir şekilde uygulamaya sokmak için izlenmesi gereken ana hareket alanları şunlardır:

- Bölümde ayrıntılı olarak incelenen teknik olanaklar, tıbbi hizmetlerin bağlama dayalı sunumu için yeterlidir. Kuşkusuz, uygulamalar sırasında bir takım yeni özellikler ve yetenekler ortaya çıkacaktır;
- Teknik olanakların başarılı bir şekilde hayata geçirilmesi için, önceliklere göre belirlenen "Biyomedikal Ontoloji" alanlarının seçilmesi önem kazanacaktır;
- "Biyomedikal Ontolojiler" alanındaki gelişmeler göz ardı edilmeden, ontoloji tabanlı uygulama geliştirme metodolojileri devreye sokulmalıdır;
- Bağlama Dayalı Yetkilendirme sorununun anlaşılır bir şekilde çözümü için, COMPRAM gibi karmaşıklık modellerinden istifade edilmelidir;
- Tanı ve tedavi süreçlerinin izlenebilmesi için anlamlı sonuç izleme metodolojileri mutlaka kullanılmalıdır. Çünkü her bir hastalığın ve problemin çözülmesi, her zaman sebep-sonuç ilişkisi çerçevesinde kapsanamayabilir. Temel amaç ve hedef, her durumda ve bağlamda daha doğru tanıların kısa zamanda konması ve daha etkili tedavilerin kolayca öngörülmesidir. Kuşkusuz bunların başarılabilmesi izlenebilir bir uygulama ile mümkün olabilecektir;

5.2 Sağlık Uygulaması – Rol ve Bağlama-Dayalı Erişim Kontrolü

Sağlık bakım etki alanındaki bir uygulama senaryosu üzerinden bağlama-dayalı erişim kontrolü sürecini kurgulamaya çalışalım.

Senaryo: *Bir hasta kalp krizi bulgusuyla hastaneye kaldırılarak büyük acil odasına getirildi. Acil servisindeki ilgili doktor, getirilen hastanın her zaman tedavi eden hekimi değildir. Ancak doktor, hastaya tıbbi müdahalede bulunabilmek için, hastanın medikal kayıtlarına okuma ve yazma yetkisiyle erişme ihtiyacı duymaktadır.*

Normalde, sadece hastayı devamlı tedavi eden hekim (müdavi hekim) hastanın medikal kayıtlarına erişim hakkına sahiptir. Bu acil servis senaryosunda, hastayı tedavi eden hekim durumunda olmayan acil servis doktorunun hastaya ait medikal kayıtlara erişmesi söz konusudur. Bu

çerçevede erişim denetiminin söz edilen senaryosuna ilişkin ilgili bağlamsal bilgiler şunlardır: acil servis doktorunun rolü “Stajyer Doktor” ve bulunduğu mekânı “Acil Odası”, hastanın o anki sağlık durumu “Kritik” ve doktorun hasta ile olan ilişkisi “Tedavi Etmeyen Hekim”. Buna ek olarak, doktorun amacı “tedavi etmek” için hastanın medikal kayıt kaynaklarına erişim isteğinde bulunmaktadır. Tüm bu faktörler dikkate alınarak erişim denetim karar işlemi gerçekleştirilmesi söz konusudur. Ayrıca durumsal değişiklikler (hastanın acil servis odasından hastanenin normal tedavi odasına taşınması gibi) olduğunda, doktorun hastanın medikal kayıt kaynaklarına olan daha fazla erişim istekleri ile ilgili erişim denetim kararları buna göre değişebilmelidir (erişim engellenmesi gibi).

Medikal kayıtların yönetimi gibi uygulama içerisinde bağlama-dayalı erişim denetimini destekleyebilmesi “kimin (kullanıcı) ne zaman (o anki bağlam) ve neden (kaynağa erişim amacı) neye (kaynaklar) erişmek istediği” gibi hususlar dikkate alınmalıdır. Böyle bir uygulama üzerinde kaynaklara erişim yönetiminde çeşitli tipteki çevre faktörlerinin değişimi erişim kontrol kararları üzerindeki etkisi söz konusudur. Bu kavramsal çerçeve, çeşitli tipteki bağlam bilgileri, amaca dayalı durumları ve bağlama-dayalı erişim kontrol politika kuralları desteklemelidir.

Bağlam bilgileri erişim denetimi karar değerlendirme sürecinde kullanılır ve ilgili varlığının durumunu belirten bilgiyi (kullanıcı, kaynak sahibi ve çevresel ortam) veya varlıklar arasındaki ilgili ilişkisel durumu tanımlar. Erişim denetimi kararları ile ilgili bağlam bilgileri üzerinde odaklanırken, bağlam varlıkları aşağıdaki şekilde kategorize edilir:

- Kullanıcı bağlamı – kullanıcı ile ilgili herhangi bir bilgi veya kaynağa erişim isteği yapan kullanıcı kimliği ve rolü;
- Kaynak bağlamı – erişilmesi istenilen kaynak özelliği ile ilgili bilgi;
- Kaynak Sahibi bağlamı – kaynak sahibi ile ilgili herhangi bir bilgi;
- Çevresel bağlam – kaynak, sahibi ve kullanıcı çevresel ortamları ile ilgili her türlü bilgi. Bunlar erişim isteği ile ilgili diğer varlıklardır.

No	Politika
1	Hastayı tedavi eden hekim, hastanın hastanedeki medikal kayıt bilgilerini okuma/yazma hakkına sahiptir. Ancak, acil bir durum söz konusu olduğunda, acil servisteki tüm stajyer doktorları, hastanın acil medikal kayıt bilgilerine erişim hakkına sahip olmalıdır.

Çizelge 5.1 Örnek Erişim Kontrolü Politikası [37]

Bağlam bilgileri, söz edilen senaryo üzerinde erişim denetim ile ilgili bağlam varlıklarını tanımlar: kullanıcıların *kimlik/rolü*, kullanıcıların bulunduğu *mekân*, kullanıcı ve hasta arasındaki *ilişki*, hastanın *sağlık durumu* v.s.

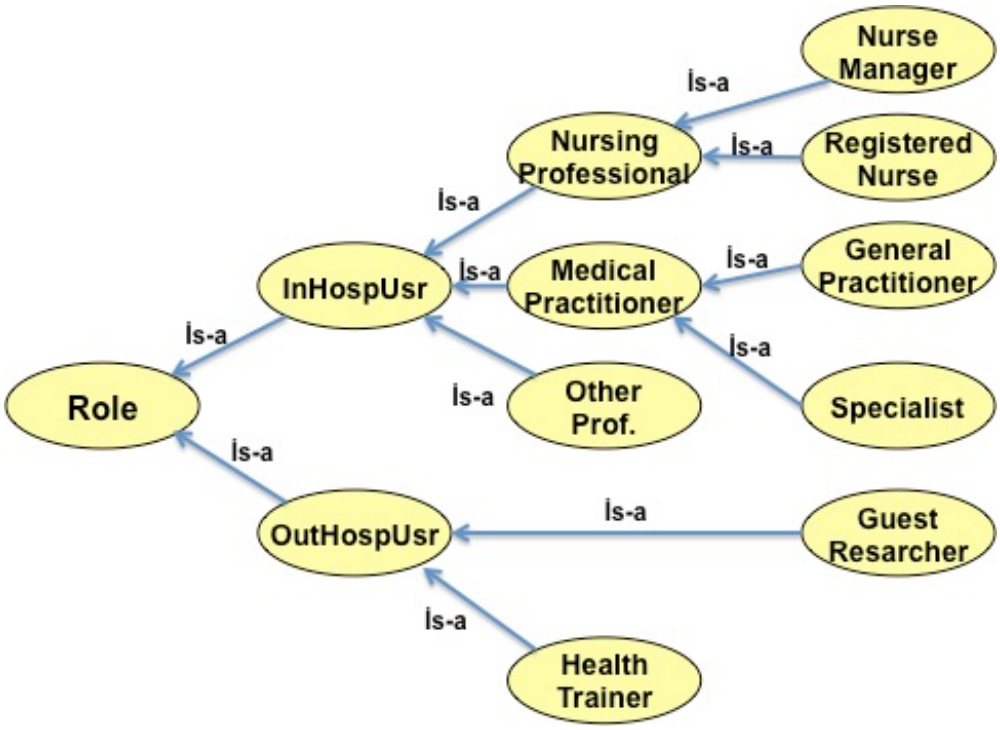
- Kullanıcı *kimliği* ve *rolü*, kullanıcıyı tanımlayan bağlam bilgisinin parçasıdır (Ali ve Stajyer Doktor). Doktorun bulunduğu *mekân* ve *erişme isteği zamanı*, kullanıcının *Mekânsal-geçici çevre* ortamlarına ilişkin bağlam bilgileridir.
- Hastanın medikal kayıtlarının *gizlilik özelliği*, *kaynak (Resource)* ile ilgili bağlam bilgilerinin parçasıdır.
- Kaynak sahibinin kimliği ve kategorisi, *kaynak sahibi (Owner)* ile ilgili bağlam bilgisinin parçasıdır.
- Hasta, erişim isteği ile ilişkili çevresel ortam varlığıdır. Hastanın bulunduğu mekân ve sağlık durumu, hastanın mekânsal ve durum bağlam bilgileri içerir.
- Doktor ve hasta arasındaki “Tedavi Etmeyen Hekim” ilişkisi, ilişkisel bağlam bilgisini tanımlar.
- Acil servis odasının durum bilgisi ise, *Mekânsal-geçici bağlam* varlığını belirler.

İlgili kullanıcılar tarafından kaynak bilgisinin ihtiyaç duyulan kısmına doğru erişim izni sağlayabilmek için kaynak bilgileri (hastanın medikal kayıtları) hiyerarşik bir şekilde ele alınmalıdır. Uluslararası uygulamalarda, hastanın sağlık sistemiyle karşılaşmasının kritik bilgileri belli bir standart çerçevede

tutulmaktadır. (Kanada: Medical Summary, Almanya Arztbrief vb…) Bu çerçevede, söz edilen senaryo ile ilgili erişim denetim politikası Çizelge 5.1'de verilmiştir. Öznenin bazı özel kaynak bilgilerine erişim sürecinde tipik politika değerlendirme işlemlerini yöneten bir üst politikanın elde edilmesi gerekir. Politika değerlendirme, PDP tarafından yorumlanarak, hedef bir kaynak üzerinde eylemi belirleyen süreçtir. Başka bir deyişle, politika değerlendirme işlemi sonucunda elde edilen politikanın kaynak üzerindeki hükmün uygulama süreci PEP tarafından gerçekleşir.

5.3 Ontoloji

Örnek senaryo ile ilgili ontoloji bileşenleri olarak bağlam varlıklarını ve bilgileri temsil eden ontoloji Şekil 4.5'te verilmiştir. Bağlam varlıkları ve bilgilerinde oluşan sınıf - alt sınıf kategorileri ve aralarındaki ilişkisel bağlantılar konusu önceki bölüm 4.2.2'de ele alınmıştır. Bağlama-dayalı erişim kontrol kararları ile ilgili bağlam bilgileri sınıflandırılması beş kategori üzerinden yapılmıştır: Bu beş kategori, "RelationshipInfo", "StatusInfo", "ProfileInfo", "LocationInfo" ve "TemporalInfo" sınıflarıdır.

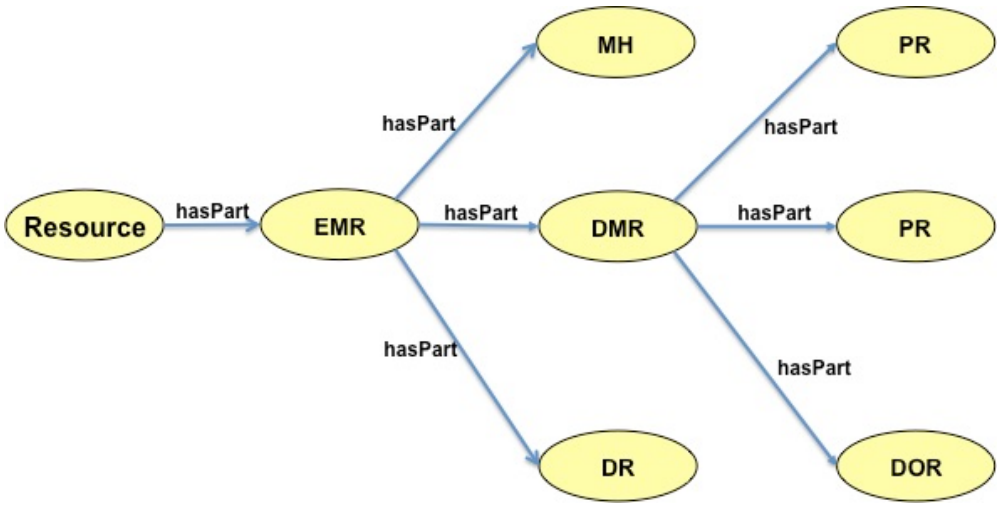


Şekil 5.1 Sağlık Etki Alanına Özgü Rol Ontolojisi [37]

Bu çerçevede, bağlam bilgisini oluşturulan alt sınıf varlıklarını şöyle bir şekilde kategorize edilir:

- Geçici bağlam – zamanı karakterize eden bilgiler (istek zamanı);
- Mekânsal bağlam – yer ve konumu karakterize eden bilgiler (bulunduğu yer);
- Durum bağlamı – o anda oluşan durumsal bilgiyi içerir (hastanın o anda sağlık durumu gibi);
- İlişkisel bağlamı - varlıklar arasındaki ilişkisel bilgiyi içerir (kullanıcı ve kaynak sahibi arasındaki ilişki, “doktor-hasta” ilişkisi);

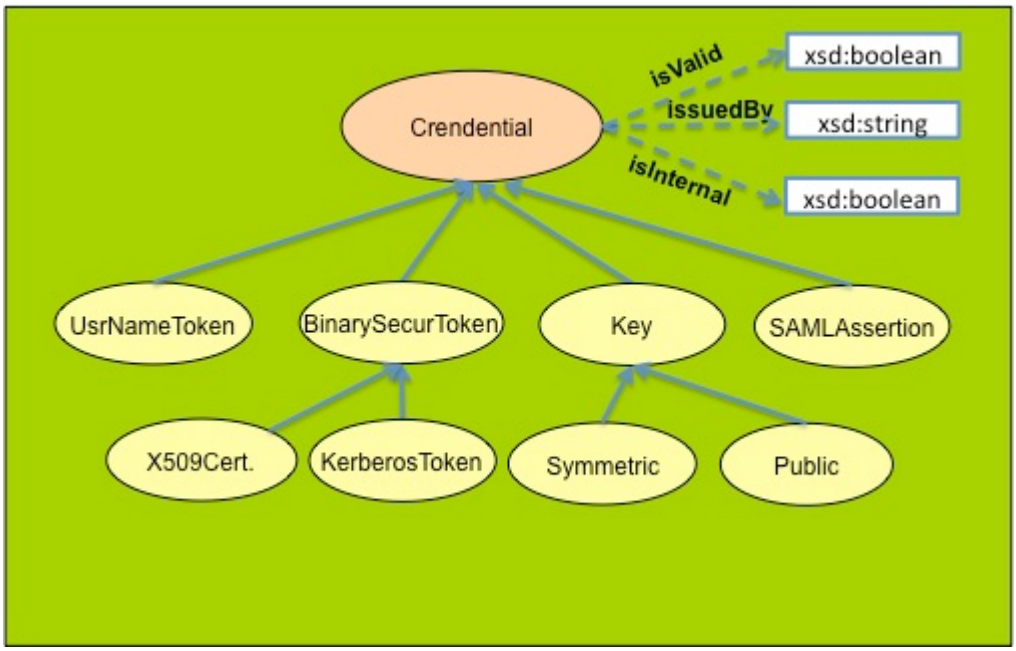
Söz edilen bağlam üst ontoloji temelinde, örnek senaryosu için etki alanına özgü ontolojilerin tanımlanması kapsamında Rol ve Kaynak ontolojilerinin belirlenmesi gerekir. Buna göre Rol, “InHospUsr” veya “OutHospUsr” olarak kategorize edilebilir. Böyle bir sınıflandırma, çeşitli tipteki (roller) kullanıcılar için farklı erişim denetimi sağlar(Şekil 5.1). Bu ontolojide, sağlık çalışanları için ASCO(Australian Standard Classification of Occupations) tarafından belirlenen standartlar temel alınarak, RBAC erişim denetiminde olduğu gibi üst-alt sınıfları arasında hiyerarşik yapıdaki erişim yetkilerinin kalıtımsal ve devir etme rol kavramına sahiptir.



Şekil 5.2 Sağlık Etki Alanına Özgü Örnek Kaynak Ontolojisi [37]

Örneğin, “Medical Practitioner” rolündeki kullanıcının hastanın günlük medikal kayıt bilgilerine erişme hakkına sahip olduğu varsayılırsa, “Specialist Practitioner” rolündeki kullanıcının da hastaya ait günlük medikal kayıt bilgilerine erişme hakkına sahip olur. Ancak, bunun tersi geçerli değildir.

Bu anlamda, semantik kurallar üzerinde rollerin dinamik atama işlemi gerçekleştirmesini sağlayacak “Kimlik” ontolojisinin kullanımı söz konusudur. Örnek olarak Şekil 5.3’te gösterildiği gibi, “Kimlik” üst sınıfı, “UsrNameToken”, “BinarySecurityToken”, “Key” ve “SAMLAssertion” alt sınıflardan oluşmaktadır. Burada, “UsrNameToken” - kullanıcı adı ve parolası kullanılarak kimlik tanımını, “BinarySecurityToken” – X.509 gibi ikili güvenlik belirteçlerle kimlik doğrulamayı, “Key” – genel veya simetrik anahtar gibi güvenlik anahtarlarla kimlik tanımını, “SAMLAssertion” ise SAML biçiminde kimlik doğrulama bilgisini ifade etmektedir. Uygulama kapsamına bağlı olarak da, “Kimlik” ontolojisi - diğer PKI alt sınıfları eklenerek daha da genişletilebilir.



Şekil 5.3 Örnek Kimlik Ontolojisi [70]

Aynı şekilde, sağlık etki alanında kaynak bilgileri (hasta kayıt verileri) hiyerarşik olarak oluşan bir ontolojiye sahiptir (Şekil 5.2). Hasta medikal kayıt yapısı, HL7 standardına göre yapılandırılmıştır. Acil medikal kayıtlar (EMR), hastanın tüm medikal kayıtlarını içerir: “Fizyolojik Kayıtlar” (PR), “Doktor Reçeteleri” (PP) ve “Günlük İnceleme Kayıtları” (DOR) gibi alt sınıflarından oluşan “Günlük Medikal Kayıtları” (DMR); “Tıbbi Geçmişi”(MH); “Demografik Kayıtları” (DR); Bu ontolojik yapıda kaynağın farklı bilgi kısımlarına erişimini düzenleyen “Bilgi Seviyesi” gibi önemli yüklem ilişkisi mevcuttur. Örneğin, senaryoya göre “Doktor” hastanın EMR kayıtlarının tüm alt bileşenlerine

erişebilirken, “Hemşire” ise sadece “Günlük Medikal Kayıtlara” erişme yetkisine sahiptir.

Özel kural dili olan SWRL kullanarak, söz edilen ontolojik kavramları ve arasındaki ilişkileri üzerindeki çıkarım kuralları tanımlanabilir. Çıkarım kuralları: $A_1 \wedge A_2 \wedge A_3, \ldots \wedge A_n \rightarrow A_1 \wedge A_2 \wedge A_3, \ldots \wedge A_r$ şeklinde tanımlanır. Burada $A_1, A_2, A_3, \ldots A_n$ giriş seviyesindeki (kuralın gövdesi) bağlamsal kavramları ve $A_1, A_2, A_3, \ldots A_r$ ise çıkarım sonuç bağlamsal kavramları (kural başlığı) temsil etmektedir [74].

Kural 1: Vücut ısısı “normal” olup da, kalp atış hızı “anormal” olursa, hastanın sağlık durumu kritik bilgisinin elde edilmesi

Owner(?o) $\wedge$ StatusInfo(?hs) $\wedge$ has(?o, ?hs) $\wedge$ ProfileInfo(?hp) $\wedge$ has(?o, ?hp) $\wedge$ bodyTemperature (?hp, “normal”) $\wedge$ heartRate (?hp, “anormal”) $\rightarrow$ healthStatus(?hs, “critical”)

Kural 2: Kullanıcıya “Medical Practitioner” rolü atanması

User(?u) $\wedge$ Role(?rol) $\wedge$ hasRole(?u, ?rol) $\wedge$ equal(?rol, “Medical Practitioner”) $\rightarrow$ assignedRole (?u, “Medical Practitioner”)

Kural 3: “Medical Practitioner” rolüne sahip kullanıcıya günlük medikal kayıt bilgilerine erişim hakkı düzenlenmesi

User(?u) $\wedge$ Role(?rol) $\wedge$ hasRole(?u, ?rol) $\wedge$ equal(?rol, “Medical Practitioner”) $\wedge$ Resource (?r) $\wedge$ hasReqRes (?u, ?r) $\wedge$ Owner (?o) $\wedge$ isOwned (?r, ?o) $\wedge$ assignedResource (?r, “DMR”) ”) $\rightarrow$ permittedResource (?u, “DMR”)

5.4 Semantik Bağlama-Dayalı Erişim Kontrolü Politikası

Durum veya bağlamlar ontoloji üzerinde düzgün tanımlanırken, bir erişim politikası ise XACML nitelikleri olarak bağlamların kullanılarak oluşturulmasıdır. Bağlama-dayalı erişim kontrolü politikası Çizelge 5.3’de bağlamlar üzerinde genişletilmiş XACML politika örneği olarak gösterilmiştir.

XACML politika dili özelliklerinde yer alan RBAC profilinde, roller özne nitelikleri olarak ifade edilmektedir. Rol nitelikleri, uygulama ortamı gereksinimlerine bağlı olarak ifade edilebilir. Genel olarak önerilen yöntemde <AttributeID “&role;”> ve rol niteliğinin ismi şeklinde kullanılması tavsiye edilir.

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
PolicySetId="PPS:Medical_Practitioner:role"
PolicyCombiningAlgId="&policy-combine;deny-overrides">
<!— Permissions for the Medical_Practitioner role —>
<Policy PolicyId="Permissions: for:the: Medical_Practitioner:role"
RuleCombiningAlgId="&rule-combine;permit-overrides">
<!— Permission to view medical record —>
<Rule RuleId="Permission:to:view:medical:record" Effect="Permit">
<Target>
<Resources>
<Resource>
        <ResourceMatch MatchId="&function;string-equal">
        <AttributeValue DataType="&xml;string">EMR</AttributeValue>
          <ResourceAttributeDesignator AttributeId="&resource;resource-id
                                                    DataType="&xml;string"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="&function;string-equal">
<AttributeValue DataType="&xml;string">read</AttributeValue>
  <ActionAttributeDesignator AttributeId="&action;action-id"
                                          DataType="&xml;string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
</Policy>
```

Çizelge 5.2 “Medical Practitioner” Rolü için Yetki İzni Politikası

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
PolicySetId="RPS:Medical_Practitioner:role"
PolicyCombiningAlgId="&policy-combine;deny-overrides">
<Target>
<Subjects>
<Subject>
 <SubjectMatch MatchId="&function;string-equal">
        <AttributeValue
        DataType="&xml;string">&roles;Medical_Practitioner </AttributeValue>
        <SubjectAttributeDesignator
         AttributeId="&role;" DataType="&xml;string"/>
 </SubjectMatch>
</Subject>
</Subjects>
</Target>
<Rule RuleId="1" Effect="Permit">
  <Target>
   <Subjects> <AnySubject/> </Subjects>
   <Resources> <AnyResource/> </Resources>
   <Action> <AnyAction/> </Action>
  </Target>
  <Condition FunctionId="string-equal">
   <Apply FunctionID="string-one-and-only">
   <SubjectAttributeDesignator
   AttributeId="inEmergency" DataType="&xml;string"/>
   </Apply>
    <Apply FunctionID="string-one-and-only">
   <ResourceAttributeDesignator
   AttributeId="inEmergency" DataType="&xml;string"/>
   </Apply>
  </Condition>
</Rule>
```

Çizelge 5.3 XACML RPS Politika Örneği

XACML için RBAC profili, rol atama belirtilmiyor ve bu işlem uygulamaya bırakılıyor. Ancak, izin atama işlemi belirtilerek ifade edilebilmektedir.

PPS (Permission Policy Set), belirli rol için izin atama işlemi için kullanılmakta ve RPS (Role Policy Set), PPS ile birlikte belirli rol niteliğini ve değeri birleştirmektedir.

PPS, kaynakları ve erişme izni verilen öznelerin eylemlerini tanımlayan <Policy> ve <Rule> bileşenleri içerir ve rol ile ilişkilendirilen tüm izinlerin kalıtımsal olarak dağılımı yapılır. Ayrıca PPS tipindeki politika içinde <Target> bileşeni kullanıyorsa, özneler için uygulanabilir <PolicySet> politikalar için kısıtlama getirilmemektedir(Çizelge 5.2). RPS ise < Target > bileşeni özneler için uygulanabilir <PolicySet> politikalar kısıtlama koşulları üzerinde gerçekleştirilmekte ve PPS referans gösterilmektedir. Bu, ek olarak, RPS içinde doğrudan bağlamsal terimler tanımlanabilmektedir. Böylece politika yönetim panelinden doğruda tanımlanmış bağlamlar üzerinde erişim denetim politikaları yazılabilir. Çizelge 5.3'te "inEmergency" bağlamı ve "Medical Practitioner" rolüne göre XACML erişim denetim politika örneği verilmiştir.

6. SONUÇ

Günümüzün bilişim dünyasında, yaygın bilgi sistemlerine odaklanmayla birlikte bilgi güvenliği ve erişim yönetimi ile ilgili önemli sorunlar ön plana çıkmıştır. Bu sistemler, sıkı güvenlik politikaları aracılığıyla bütünlüğün ve gizliliğin korunduğu bilgi kaynaklarına “her zaman, her yerden ve her şekilde” temelinde şeffaf erişmeye olanak tanımalıdır. Böyle bir erişilebilirliğin beklentileri karşılayabilmesi adına erişim denetim düzeneklerinin modellenmesi yönünde yapılan araştırma çalışmaları üç ana yönde yürütülmektedir: Birincisi, kullanıcı bağlamı temelinde karar verme düzeneğini uyarlayan bağlama-dayalı erişim kontrolü modellerine doğru kaymadır. İkincisi, duruma dayalı ve kritik ortamda esnek karar verme çözümleri üzerine odaklanmasıdır. Üçüncüsü ise dağıtık bir ortamda farklı etki alanında bulunan yetkilendirme sistemlerinin anlayabileceği biçimde erişim denetimi politika modellerinin ortaya konulmasıdır.

Sonuçta, kimlik tanıma veya rol tabanlı erişim kontrolü modellerinden bağlama dayalı yaklaşımlara doğru yönelen yeni yetkilendirme modeli çözümlerine ihtiyaç duyulmaktadır. Bu tez çalışmasında, bir örnek RBAC modeli üzerinden anlamsal ontolojik tekniklerle bağlama-dayalı erişim denetimi düzeneği birleştirilerek, yeni bir kavramsal model sunulmuştur. Bu çerçevede, bağlamsal bilgileri anlamsal olarak temsil eden bağlam ontolojisi ve durumsal bir ortamda erişim denetimi politikasını ifade eden politika ontolojisi kurgulanmıştır.

Sunulan model ve sistem mimarisi, gerçek zamanlı sistemlerde erişim denetim politikalarının anlamsal ontoloji modelleme yönetimiyle ifade edilerek, esnek ve güvenli bir yetkilendirme düzeneğinin önemini vurgulamıştır. Bu tezin önemli amaçlarından biri de, bağlama dayalı erişim denetiminde semantik kullanımın uygulanabilirliğini göstermektir ve XACML özelliğini kullanarak, semantik bağlamların erişim denetim politikasına entegrasyonu söz konusudur. Burada asıl amaç, bağlamın oluşturularak semantik olarak nasıl ifade edebildiğini ve bunun XACML genişletileme yöntemiyle erişim denetim politikasına entegrasyon yapılabildiğini göstermektir.

Bu anlamda, durum ve çevre etkenlerine göre oluşan değişken bağlam bilgilerinin modellenmesi ve anlamsal olarak ifade edilmesi, ayrıca bir erişim denetim politikasına entegrasyonu sağlayan örnek bir model kurgusu yapılmıştır. Aynı zamanda RBAC gibi farklı erişim denetim modelleri üzerinde anlamsal bağlam modellemenin uygulanabilirliği gösterilmiştir. Böylece rol kavramlarının bağlam modelleme yoluyla ifade edilebildiği ortaya konulmuştur. Bu ise politika belirlemede roller ve bağlamlar olmak üzere her ikisini de kullanan bir XML tabanlı erişim denetim politikası sunumuna olanak vermektedir.

Durum ve çevre etkenlerinin ağ bağlamında olay tabanlı olarak ele alınmasıyla güvenlik düzeyinin artırılmasına yönelik karmaşık olay işleme tekniklerinin uygulanmasına olanak sağlanmaktadır. Bu yeni güvenlik düzeyi günümüzde ağ güvenliği uzmanları tarafından manuel olarak uygulanmakta olan güvenliği negatif yönde etkileyen olay örüntülerinin ortaya çıkarılması işlemlerinin otomatik hale getirilmesini sağlayacaktır. Bu sayede günümüzde gözden kaçırılması mümkün olan bazı güvenlik açıklarının gerçek zamanlı olarak ortaya çıkarılması sağlanacaktır. Karmaşık olay işleme kullanılarak ağ güvenliğinin iyileştirilmesi bu tezde ortaya konulan çalışmaların devamı niteliğinde olacaktır.

KAYNAKLAR

[1] Mark Weiser, "Hot Topics: Ubiquitous Computing" *IEEE Computer*, October 1993.

[2] http://en.wikipedia.org/wiki/Policy Retrieved on 07.09.2010.

[3] R. Chadha and L. Kant. Policy-Driven Mobile Ad hoc Network Management. Wiley-IEEE Press, 2007.

[4] N. Damianou, A. Bandara, M. Sloman, and E. Lupu. A Survey of Policy Specification Approaches, 2002.

[5] N. Damianou, N. Dulay, E. Lupu, and M. Sloman. The Ponder Policy Specification Language. In Lecture Notes in Computer Science, pages 18{38. Springer-Verlag, 2001.

[6] H. Janicke. The Development of Secure Multi-Agent Systems. PhD thesis, De Montfort Univeristy, 2007.

[7] T. Strang and C. Linnhoff-Popien. A Context Modeling Survey. In In: Work-shop on Advanced Context Modelling, Reasoning and Management, UbiComp 2004 - The Sixth International Conference on Ubiquitous Computing, Notting- ham/England, 2004.

[8] A. K. Dey. Understanding and using context. Personal Ubiquitous Comput., 5(1):4–7, Jan. 2001.

[9] N. Li. How to make discretionary access control secure against trojan horses. In Parallel and Distributed Processing, 2008. IPDPS 2008. IEEE International Symposium on, pages 1–3, 2008.

[10] R. Nick, J. Pascoe, and D. Morse. Enhanced reality fieldwork: the context-aware archaeologist assistant. In Exon, editor, Computer Applications & Quantitative Methods in Archaeology, volume 0. Archaeopress, 1997.

[11] J. Park and R. Sandhu. Towards usage control models: beyond traditional access control. In Proceedings of the seventh ACM symposium on Access control models and technologies, SACMAT ’02, pages 57–64, New York, NY, USA, 2002. ACM.

[12] M. J. Pascoe. Adding generic contextual capabilities to wearable computers. In Proceedings of the 2nd IEEE International Symposium on Wearable Computers, ISWC ’98, pages 92, Washington, DC, USA, 1998. IEEE Computer Society.

[13] R. Sandhu and J. Park. Usage control: A vision for next generation access control. In V. Gorodetsky, L. Popyack, and V. Skormin, editors, Computer Network Security, volume 2776 of Lecture Notes in Computer Science, pages 17–31. Springer Berlin Heidelberg, 2003.

[14] R. Sandhu and P. Samarati. Access control: principle and practice. Communications Magazine, IEEE, 32(9):40–48, 1994.

[15] B. Schilit and M. Theimer. Disseminating active map information to mobile hosts. Network, IEEE, 8(5):22–32, 1994.

[16] P. Schneck. Persistent access control to prevent piracy of digital information. Proceedings of the IEEE, 87(7):1239–1250, 1999.

[17] F. Siewe, A. Cau, and H. Zedan. A compositional framework for access control policies enforcement. In Proceedings of the 2003 ACM workshop on Formal methods in security engineering, FMSE ’03, pages 32–42, New York, NY, USA, 2003. ACM

[18] Brown, M. Supporting User Mobility. International Federation for Information Processing (1996).

[19] Cooperstock, J., Tanikoshi, K., Beirne, G., Narine, T., Buxton, W. Evolution of a Reactive Envi ronment CHI ’95 (1995) 170-177.

[20] Dey, A.K., Abowd, G.D., Wood, A. CyberDesk: A Framework for Providing Self-Integrating Context-Aware Services. Knowledge-Based Systems, 11 (1999) 3-13.

[21] Elrod, S., Hall, G., Costanza, R., Dixon, M., des Rivieres, J. Responsive Office Environments. CACM 36(7) (1993) 84-85.

[22] Fickas, S., Korteum, G., Segall, Z. Software Organization for Dynamic and Adaptable Wearable st Systems. 1 International Symposium on Wearable Computers (1997) 56-63.

[23] Hull, R., Neaves, P., Bedford-Roberts, J. Towards Situated Computing. 1 International Symposium on Wearable Computers (1997) 146-153 7.

[24] Rekimoto, J., Ayatsuka, Y ., Hayashi, K. Augment-able Reality: Situated Communication through nd Physical and Digital Spaces. 2 International Symposium on Wearable Computers (1998) 68-75.

[25] Salber, D., Dey, A.K., Abowd, G.D. Ubiquitous Computing: Defining an HCI Research Agenda for an Emerging Interaction Paradigm. Georgia Tech GVU Technical Report GIT-GVU-98-01 (1998).

[26] Schilit, B., Theimer, M. Disseminating Active Map Information to Mobile Hosts. IEEE Network, 8(5) (1994) 22-32.

[27] Want, R., Hopper, A., Falcao, V., Gibbons, J. The Active Badge Location System. ACM Transactions on Information Systems 10(1) (1992) 91-102.

[28] J. B. Filho and H. Martin. A generalized context-based access control model for pervasive environments. In Proceedings of the 2nd SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS, SPRINGL ’09, pages 12–21, New York, NY, USA, 2009. ACM.

[29] AKMAN, V., AND SURAV , M. The use of situation theory in context modeling. Computational Intelligence 13 , 3 (1997), 427–438.

[30] BARWISE, J., AND PERRY , J. Situations and Attitudes . MIT Press, 1983.

[31] CHEN, H., FININ , T., AND JOSHI , A. Using OWL in a Pervasive Computing Broker. In Proceedings of Workshop on Ontologies in Open Agent Systems (AAMAS 2003) (2003).

[32] GHIDINI, C., AND GIUNCHIGLIA , F. Local models semantics, or contextual reasoning=locality+compatibility. Artificial Intelligence 127 , 2 (2001), 221–259.

[33] GIUNCHIGLIA, F. Contextual reasoning. Epistemologica - Special Issue on I Linguaggi e le Macchine 16 (1993), 345–364. Also IRST-Technical Report 9211-20, IRST, Trento, Italy.

[34] GRAY, P., AND SALBER , D. Modelling and Using Sensed Context Information in the design of Interactive Applications. In LNCS 2254: Proceedings of 8th IFIP International Conference on Engineering for Human-Computer Interaction (EHCI 2001) (Toronto/Canada, May 2001), M. R. Little and L. Nigay, Eds., Lecture Notes in Computer Science (LNCS), Springer, p. 317 ff.

[35] GU , T., WANG , X. H., PUNG , H. K., AND ZHANG , D. Q. Ontology Based Context Modeling and Reasoning using OWL. In Proceedings of the 2004 Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS2004) (San Diego, CA, USA, January 2004).

[36] INDULSKA, J., ROBINSONA , R., RAKOTONIRAINY , A., AND HENRICKSEN , K. Experiences in using cc/pp in context-aware systems. In LNCS 2574: Proceedings of the 4th International Conference on Mobile Data Management (MDM2003) (Melbourne/Australia, January 2003), M.-S. Chen, P. K. Chrysanthis, M. Sloman, and A. Zaslavsky, Eds., Lecture Notes in Computer Science (LNCS), Springer, pp. 247–261.

[37] Kayes, A.S.M., Han, J. N & Colman, A. An ontology-based approach to context-aware access control for software services. 14th International Conference on Web Information System Engineering (WISE 2013), pp. 410–420. Springer Berlin, 2013.

[38] MC CARTHY, J., AND BUVAĞ. Formalizing context (expanded notes). In Working Papers of the AAAI Fall Symposium on Context in Knowledge Representation and Natural Language (Menlo Park, California, 1997), S. Buvağ and Ł. Iwanska, Eds., American Association for Artificial Intelligence, American Association for Artificial Intelligence, pp. 99–135.

[39] ÖTZTÜRK, P., AND AAMODT, A. Towards a model of context for case-based diagnostic problem solving. In Context-97; Proceedings of the interdisciplinary conference on modeling and using context (Rio de Janeiro, February 1997), pp. 198–208.

[40] STRANG, T. Service Interoperability in Ubiquitous Computing Environments . PhD thesis, Ludwig-Maximilians-University Munich, Oct. 2003.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] MotOrBAC. 2009. http://motorbac.sourceforge.net.

[46] Ryan, N., Pascoe, J., Morse, D. Enhanced Reality Fieldwork: The Context-Aware Archaeological Assistant. Gaffney,V., van Leusen, M., Exxon, S. (eds.) Computer Applications in Archaeology (1997).

[47] Schilit, B., Adams, N. Want, R. Context-Aware Computing Applications. 1 International Workshop on Mobile Computing Systems and Applications. (1994) 85-90.

[48] E. Bertino, P. A. Bonatti, and E. Ferrari. Trbac: A temporal role-based access control model. ACM Trans. Inf. Syst. Secur., 4(3):191–233, Aug. 2001.

[49] L. Chen and J. Crampton. On spatio-temporal constraints and inheritance in role-based access control. In Proceedings of the 2008 ACM symposium on Information, computer and communications security, ASIACCS '08, pages 205–216, New York, NY, USA, 2008. ACM.

[50] K. Thi, T. Dang, P. Kuonen, and H. Drissi. Strobac: Spatial temporal role based access control. In Computational Collective Intelligence. Technologies and Applications, volume 7654 of Lecture Notes in Computer Science, pages 201–211. Springer Berlin Heidelberg, 2012.

[51] E. Uzun, V. Atluri, S. Sural, J. Vaidya, G. Parlato, A. L. Ferrara, and M. Parthasarathy. Analyzing temporal role based access control models. In Proceedings of the 17th ACM symposium on Access Control Models and Tech- nologies, SACMAT '12, pages 177–186, New York, NY, USA, 2012. ACM.

[52] G. Zhang and M. Parashar. Dynamic context-aware access control for grid applications. In Grid Computing, 2003. Proceedings. Fourth International Work- shop on, pages 101–108, 2003.

[53] H. Zhang, Y. He, and Z. Shi. Spatial context in role-based access control. In Proceedings of the 9th international conference on Information Security and Cryptology, ICISC'06, pages 166–178, Berlin, Heidelberg, 2006. Springer- Verlag.

[54] Mohammed H. Al-Sammarraie. Policy-based Approach for Context-aware Systems. PhD thesis, De Montfort Univeristy, 2011.

[55] Internet Engineering Task Force (IETF) http://www.ietf.com Retrieved on 10.02.2011.

[56] W. Dargie. Context-Aware Computing and Self-Managing Systems. Chapman & Hall/CRC, 1st edition, 2009.

[57] S.Godik and T.Moses. OASIS extensible access control markup language (xacml) version 2.0. Technical report, OASIS, February 2005.

[58] Kulkarni, D., Tripathi, A.: Context-aware role-based access control in pervasive computing systems. In: SACMAT. pp. 113-122 (2008).

[59] Toninelli, A., Montanari, R., Kagal, L., Lassila, O.: A semantic context-aware access control framework for secure collaborations in pervasive computing environments. In: ISWC. pp. 473-486 (2006).

[60] Hulsebosch, R.J., Salden, A.H., Bargh, M.S., Ebben, P.W.G., Reitsma, J.: Context sensitive access control. In: SACMAT. pp. 111-119 (2005).

[61] Corradi, A., Montanari, R., Tibaldi, D.: Context-based access control management in ubiquitous environments. In: NCA. pp. 253-260 (2004).

[62] A. Dersingh, R. Liscano, and A. Jost, “Context-aware access control using semantic policies,” In Ubiquitous Computing And Communication Journal Special Issue of Autonomic Computing Systems and Applications, 2008,pp. 1-14.

[63] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila, “A semantic context aware access control framework for secure collaborations in pervasive computing environments,” In proceedings of the 2006 International Semantic Web Conference, 2006, pp. 473–486.

[64] A. Naumenko, S. Srirama, and V. Terziyan, “Semantic authorization of mobile web services,” Journal of Theoretical and Applied Electronic Commerce Research, vol. 1, no. 1, 2006, pp. 1-15.

[65] A.E. Moussa, A. Morteza, and J. Rasool, “Handling context in a semantic based access control framework,” In proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops, IEEE Computer Society, 2009, pp. 103-108.

[66] L.Kagal, “A Policy-Based Approach to Governing Autonomous Behavior in Distributed Environments”, Dissertation, 2004.

[67] L. Kagal, and T. Berners-Lee, “Rein: Where policies meet rules in the semantic web,” Technical report, MIT, 2005.

[68] E. Damiani, S. De Capitani di Vimercati, C. Fugazza, and P. Samarati, “Extending Policy Languages to the Semantic Web”, International Conference on Web Engineering (ICWE2004), Lecture Notes in Computer Science, pp. 330-343, July 2004.

[69] T. Priebe, W. Dobmeier, and N. Kamprath, “Supporting Attribute-based Access Control with Ontologies,” First International Conference on Availability, Reliability and Security (ARES'06), pp. 465-472, 2006.

[70] He, Z., Wu, L., Li, H., Lai, H., Hong, Z.: Semantics-based access control approach for web service. JCP 6(6), 1152-1161 (2011).

[71] S.Verma, S. Kurma, L., M. Singh : Hybrid Access Control Model in Semantic Web. IJCSNS, VOL.13 No. 6, pp. 92-97 JUNE 2013.

[72] Dana Al Kukhun, Steps Towards Adaptive Situation and Context-Aware Access: A Contribution to the Extension of Access Control Mechanisms within Pervasive Information Systems. PhD thesis, de Toulouse University, Oct. 2012.

[73] M. Knechtel, J. Hladik, “RBAC Authorization Decision with DL Reasoning”, In Proceedings of the IADIS International Conference WWW/Internet, 2008, pp.169-176.

[74] W3C, “SWRL: A Semantic Web Rule Language Combining OWL and RuleML”, http://www.w3.org/Submission/SWRL/, 2004.

[75] Kagal, L. , Finin, T. , Joshi, A. , Niu, J. , Sandhu, R. , and Winsborough, W. ROWLBAC -Representing Role Based Access Control. in OWL' Proceedings of SACMAT’08 . Estes Park, Colorado, USA, 2008.

[76] He, Z.Q., Huang, K.Y., Wu, L.F.: Using semantic Web techniques to implement access control for web service. In: The International Conference on Information Computing and Applications (ICICA 2010) 2010, pp. 258–266. IEEE Press, New York (2010).

[77] Shen, H.B., Cheng, Y.: A semantic-aware context-based access control framework for mobile web services. In: The 3rd International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC 2011 (2011).

[78] C. Cocos and W. MacCaull, An Ontological Implementation of a Role-Based Access Control Policy for Health Care Information, in H. Herre, R. Hoehndorf, J Kelso and S. Schulz(eds.), OBML 2010 Workshop Proceedings, IMISEREPORT Nr. 2/2010, http://www.ontomed.de/obml/ws2010/obml2010report.pdf, 2010.

[79] E. Uzun, V. Atluri, S. Sural, J. Vaidya, G. Parlato, A. L. Ferrara, and M. Parthasarathy. Analyzing temporal role based access control models. In Proceedings of the 17th ACM symposium on Access Control Models and Technologies, SACMAT ’12, pages 177–186, New York, NY, USA, 2012. ACM.

[80] R. Sandhu, X. Zhang, K. Ranganathan, and M. J. Covington. Client-side access control enforcement using trusted computing and pei models. Journal of High Speed Networks, 15(3), May 2010.

[81] J. Zheng, kun Zhang, wen Zheng, and an Tan. Dynamic role-based access control model. Journal of Software, 6(6), 2011

[82] H. Wang, Y. Zhang, and J. Cao. Access control management for ubiquitous computing. Future Generation Computer Systems, 24(8):870 – 878, 2008.

[83] K. Thi, T. Dang, P. Kuonen, and H. Drissi. Strobac: Spatial temporal role based access control. In Computational Collective Intelligence. Technologies and Applications, volume 7654 of Lecture Notes in Computer Science, pages 201–211. Springer Berlin Heidelberg, 2012.

[84] M. A. Luo Xiaofeng, Li Ling and L. Wanbo. The contextual usage control model. Zhejiang University Science (Computers & Electronics), 2012.

[85] Carlisle Adams. Authorization Architecture, Encyclopedia of Cryptography and Security, pages 23-27, Springer US, 2005.

[86] Özgü CAN, Murat Osman ÜNALIR. Ontoloji Tabanlı Erişim Denetimi (Ontology Based Access Control), Pamukkale Üniversitesi, Mühendislik Bilimleri Dergisi, Cilt 16, Sayı 2, Sayfa 197-206, 2010.

[87] Ganesh Godavari and Edward Chow, "Secure Information Sharing Using Attribute Certificates and Role Based Access Control", In Proceedings of Security and Management'2005, pp: 269-276, 2005.

[88] Trent Jaeger, Elena Ferrari: SACMAT 2004, 9th ACM Symposium on Access Control Models and Technologies, Yorktown Heights, New York, USA, June 2-4, 2004, Proceedings. ACM 2004, ISBN 1-58113-872-5.

[89] S. LOKE. Context-Aware Pervasive system: Architectures for new breed of applications. Auerbach Publications, Wiley, 2006

[90] C. dong Wang, T. Li, and L.-C. Feng. Context-aware environment-role-based access control model for web services. In Multimedia and Ubiquitous Engineering, 2008. MUE 2008. International Conference on, pages 288–293, 2008

[91] MC CARTHY, J. Notes on formalizing contexts. In Proceedings of the Thirteenth International Joint Conference on Artificial Intelligence (San Mateo, California, 1993), R. Bajcsy, Ed., Morgan Kaufmann, pp. 555–560.

ÖZGEÇMİŞ

Kimlik Bilgileri

Adı Soyadı:	Dilmurod VAHABDJANOV
Doğum Yeri:	Özbekistan
Medeni Hali:	Evli
E-posta:	dil@hacettepe.edu.tr
Adresi:	Hilal Mah. 687. Sok. 15/4 Yıldız Çankaya Ankara

Eğitim

Lisans:	Andijan Devlet Ünv. Matematik Ve Enformatik Böl., Özbekistan, 1992
Yüksek Lisans:	Hacettepe Ünv. Bilgisayar Müh. Böl., Ankara, 1998, Tez Konusu: Bilgisayar Ağları Üzerinden Sesli Mesaj Aktarım Sistemi Tasarımı ve Gerçekleştirimi
Doktora:	Hacettepe Ünv. Bilgisayar Müh. Böl., Ankara, 2015 Tez Konusu: Bağlama Dayalı Rol Tabanlı Yetkilendirmede Semantik Model Kullanarak Erişim Denetimi ve Yönetimi: Sağlık Alanı için Bir Durum Çalışması

Yabancı Dil ve Düzeyi

İngilizce:	İyi
Rusça	iyi

İş Deneyimi

Kurum:	Hacettepe Üniversitesi BİDB, ANKARA
Pozisyon/Süre:	Sistem ve Ağ Yöneticisi – 1997 - 2005
Teknolojiler:	ATM, IDS, IPS, Firewall, VTYS, Felaket Kurtarma Merkezi, WIMAX, Güvenli mobil iletişim.

Sorumluluklar: Kurumunun sistem ve iletişim ağ alt yapılarının güvenliği sağlanması, veri kayıbını aza indirilmesi amacıyla FKM süreçlerin yönetimi ve denetimi.

Kurum: Hacettepe Üniversitesi Hastaneleri, ANKARA
Pozisyon/Süre: Sistem ve Ağ Yöneticisi – 1998-2007
Teknolojiler: HIS, LIS, PACS, PYXIS, SAN, FKM, Güvenli Mobil iletişimi.
Sorumluluklar: Kurumunun bilişim hizmetleri ve iletişim ağ alt yapıları ve veri güvenliği sağlanması, hastane bilişim hizmetlerin sürekli erişilebilirliğinin sağlanması amacıyla FKM süreçlerin yönetimi ve denetimi, ayrıca sistemlerde bulunan zafiyetlerin tespiti ve yönetimi.

Kurum: Çankaya Belediyesi, ANKARA
Pozisyon/Süre: Sistem ve Ağ Güvenliği Danışmanı – 2006 - 2008

Kurum: GenPower Jeneratör Genel Müdürlüğü, ANKARA
Pozisyon/Süre: Bilişim Hizmetleri Danışmanı – 2011 – 2012

Kurum: Hacettepe Üniversitesi BİDB, ANKARA
Pozisyon/Süre: Sıhhiye Birimi Sorumlusu – 2007
Teknolojiler: ATM, IDS, IPS, Firewall, VTYS, Felaket Kurtarma Merkezi, WIMAX, Güvenli mobil iletişim.
Sorumluluklar: Kurumunun Sıhhiye yerleşkesinin iletişim ağ alt yapıları güvenliği ve bilişim hizmetlerinin kesintisiz çalışmasını sağlanması.

Deneyim Alanları

Programlama: C, C++, Borland Delphi, ADA, JEE, çeşitli Web teknolojileri ve uygulama çatıları.
İletişim Sistemleri: MS Windows Server tüm türevleri, UNIX (AIX, Tru64, Sun, Novel, HP-UX), Linux çeşitli dağıtımları.

Sistem ve Ağ: LAN/WAN Mimarileri, TCP/IP Soket programlama, IDS, IPS, güvenlik duvarları, LDAP, AD yetkilendirme mimarileri, güvenlik modelleri ve araçları

Veri tabanı: Oracle, Sybase, Postgres, MySQL, PL/SQL, MSSQL

Tezden Üretilmiş Projeler ve Bütçesi

-

Tezden Üretilmiş Yayınlar

Erzurumlu K, Eryılmaz E.N, **Vahabdjanov D**, Saatci A. A Requirements Consolidation and Customisation Framework for Patient Safety Oriented Distributed Access Control Models: An Ontological Approach. Libre Software Meeting for Medicine, July 5-9, 2005, Dijon, Fransa, Özet.

Vahabdjanov D, *Erzurumlu K*, Çitak M, Solmaz B. Open Source Software Usage on Municipalities; A Case Study: Çankaya Municipality. Procedia-Computer Science Journal, 2011, Volume 3, 805-808

Tezden Üretilmiş Tebliğ ve/veya Poster Sunumu ile Katıldığı Toplantılar

-