T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL İMZADA KURUMSAL YETKİ MODELİ

ALPER UĞUR
DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE
2016

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL İMZADA KURUMSAL YETKİ MODELİ

ALPER UĞUR
DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMANI
PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE
2016

T.R.

GEBZE TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

INSTITUTIONAL AUTHORIZATION MODEL ON DIGITAL SIGNATURES

ALPER UĞUR

A THESIS SUBMITTED FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER ENGINEERING

THESIS SUPERVISOR

PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE

2016

GEBZE TEKNİK ÜNİVERSİTESİ	**DOKTORA JÜRİ ONAY FORMU**

GTÜ Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 27./06./2016 tarih ve 2016./43.. sayılı kararıyla oluşturulan jüri tarafından 28/07/2016 tarihinde tez savunma sınavı yapılan ALPER UĞUR 'un tez çalışması Bilgisayar Mühendisliği Anabilim Dalında DOKTORA tezi olarak kabul edilmiştir.

JÜRİ

ÜYE (TEZ DANIŞMANI)	: PROF. DR. İBRAHİM SOĞUKPINAR
ÜYE	: PROF. DR. H. ALİ MANTAR
ÜYE	: PROF. DR. VEDAT COŞKUN
ÜYE	: DOÇ. DR. MEHMET GÖKTÜRK
ÜYE	: YRD. DOÇ. DR. MURAT AYDOS

ONAY

Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun

……./……./..…… tarih ve ……../…..... sayılı kararı.

İMZA/MÜHÜR

ÖZET

Kurumsal iş akışında belgeler, oluşturulup işlenmekte, kurum içi veya kurumlar arası süreçlerde kullanılmakta ve arşivlenmektedirler. Kurumsal yapı, farklı yetki seviyelerine sahip birimlerin, iş akışında tanımlı fonksiyonlarını yerine getirmeleri üzerine bina edilmiştir. Yetki denetim sistemleri, kurumdaki kullanıcının, sadece ait olduğu fonksiyonel gruba tanımlanan izinler doğrultusunda işlem yapabilmesine olanak tanımalıdır. Kurumsal iş akışı ve bilgi sistemlerinde, yetki denetimi için, literatürde birçok mekanizma ve yöntem yer almaktadır. Yetki denetim mekanizmalarının, iş akışı süreci kapsamında uygulanmasında eksikliklerinin olduğu gözlenmektedir. Temel oturum açma mekanizması, tek başına uygulandığında sistem genelinde yetki izni sağlarken; bir başka yetki denetim yöntemi olan erişim denetim listeleri, yetkiler için kısıtlı sınırlama ve tanımlama olanağı sağlayabilmektedir. Rol tabanlı yetki denetimleri ise kurumsal iş akışında yönergeleri karşılayamamaktadır. Kurum içi iş akışında uygulanan yetki denetimi, kurumlar arası yazışmalar gibi kurum yapısı dışına çıkan süreçlerde de yetersiz kalmaktadır. Bu çalışmada, katmanlı bir yetki modeli önerilerek yetki denetim mekanizmaları için karşılaştırmalı ve bütünsel bir analiz yapısı sunulmaktadır. Önerilen model, yetki denetim mekanizmalarının özniteliklerini ortaya koyarak, yöntemler için yetenekleri ve katkılarına göre analiz ve sonuç çıkarımı imkânı sağlamaktadır. Model, kurumsal yetki uygulamalarında kapsamın belirlenmesi ve gereksinimler dâhilinde eksikliklerin çıkarılması ve çözümlenmesi için bir rehber olabilecektir. Bu çalışmada, yetki denetiminin analizi, Petri ağları yöntemi ile ortaya konulmuştur. Kurumsal yetki denetimindeki eksiklikler için sayısal imza üzerinde bir vaka çalışması yapılmış ve yetki denetiminin kurumsal yönergeleri de kapsayacak şekilde genişletilerek imzanın yetki denetimi işleviyle donatıldığı bir çözüm modeli de önerilmiştir. Bu çözüm, eşleme tabanlı kriptografi ile gerçeklenmiş ve yapılan analizler çalışmaya dâhil edilmiştir.

Anahtar Kelimeler: Yetki Denetim Mekanizmaları, Kurumsal Yetki Denetimi, Petri Ağları, Sayısal İmza, Eşleme Tabanlı Kriptografi, Katmanlı Yetki Denetim Modeli(KYED)

SUMMARY

In the institutional workflow, documents are created, processed in internal or external operations and archived. Institutional structure is based on different business units those achieve their various functionalities defined in the workflow. The authorization systems must enable institutional user, perform operations by only the permissions which were defined for the functional unit he belongs. There are various methods proposed in literature to provide authorization control in workflows and information systems. The authorization implementations have deficiencies based on procedural scope. Basic login mechanisms grant system-wide access; the provided margins are broad. Access control lists provide limited definition on restrictions. Role based authorizations do not cover regulations in institutions where regulations in institutional workflow. The authorization mechanisms implemented for the workflow may cover internal correspondences but there exists deficits in external operations. The proposed multi-layer authorization model depicts the attributes of authorization mechanisms and analyzes the methods according to their authorization capabilities and contributions to the reliability of documents in workflow. The layered structure provides comparative and integrated analysis of the authorization mechanisms. The incremental authorization structure would be a guide for implementations that each layer presents scope of authorization by providing analysis on deficiencies and the methods of solution. The analysis of authorization mechanisms are introduced with Petri net analysis. Furthermore, a case study on digital signature for the deficiencies of authorization on institutional workflow is presented and an institutional authorization mechanism on documents is also proposed. The proposed mechanism suggests and implements an authorization mechanism to enclose authorization restrictions in institutional regulations. The mechanism is implemented using pairing based cryptography and the analyses are provided.

Key Words: Authorization Mechanisms, Institutional Authorization, Petri Nets, Digital Signature, Pairing Based Cryptography, Layered Authorization Model for System Security (LAMSSE)

TEŞEKKÜR

Başta, tez çalışmamın başarısının arkasındaki isim, değerli danışmanım Sayın. Prof. Dr. İbrahim SOĞUKPINAR'a, tezime yaptıkları önemli katkılardan ötürü değerli tez jürime teşekkürlerimi sunarım.

Yaptığım her iyi işin müsebbibi olan ve bu dünyayı yaşanılır kılan, çok sevgili aileme ise ne kadar teşekkür etsem az gelecek, biliyorum. Bu tez çalışmamı, onlarla geçirmem gereken zamanı, yaptığım çalışmalara harcadığımda, gösterdikleri sabır ve destek için o güzel insanlara adıyorum.

Eşim Belgin'e, sana masallar yazmam gereken zamanı tez, makale ve bildirilere harcadım.

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler ve Kısaltmalar		Açıklamalar
ABAC	:	Attribute Based Access Control
AVBYS	:	Arşiv ve Belge Yönetim Sistemi
BBYS	:	Bilgi ve Belge Yönetim Sistemi
KDC	:	Key Distribution Center
OAuth	:	Ongoing Authorization
RADIUS	:	Remote Authentication and Dial-In User Service
RBAC	:	Role Based Access Control
SoD	:	Seperation of Duties

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

1. GİRİŞ

Güvenlik politikaları ve imza yetkisi yönergeleri, kurumsal iş akışında, belgeler üzerinde, yetki sınırlarını tanımlayan yazılı temel kuralları oluşturur. Kurumsal iş akışında, yönergelere göre hazırlanan belgelerin, güvenliği ve geçerliliği bu mekanizmaların, işlevlerini tam olarak yerine getirmelerine bağlıdır. Kurumsal yazışmalarda belgeler, kurumsal yetkilere sahip birimler tarafından oluşturulmakta veya onaylanmaktadır. Belgeler üzerinde yetki dâhilinde yapılan bu işlemler ilgili belgeyi geçerli kılmaktadır.

Uygulamalarda, sistem giriş yetkisinden erişim denetimine kadar, birçok gelişmiş yetkilendirme mekanizması kullanılmaktadır. Bu mekanizmalar, iş akışında, varlıkların sürece dâhil olup olamayacağına karar veren yöntemlerden oluşurlar. Bu yaklaşım ile iş akışındaki işlemler üzerinde anlık yetki denetimi gerçekleştirilmektedir. Kullanıcıya, ona özgü tanımlanmış ayrıcalıkların belirlediği sınırlar çerçevesinde işlem yapma izni verilir. Bu denetime tabi olan işlemler, yetki çerçevesinde gerçeklenmiş olarak kabul edilmektedir. Oysa gerçeklenen kontrol yaklaşımı, süreçte, yetki denetiminin sürdürülebilirliğini etkilemektedir.

Kullanılan yetki denetim mekanizmaları, temel problemlerin çözümlerini adreslerken başka denetim problemlerine karşı zayıflık göstermektedirler. Bu mekanizmalar ve zayıflıklarına aşağıda kısaca değinilmektedir.

- Kimlik doğrulama, sistemin erişim yetkisini denetlemek için kullanılır. İstemci, kimlik ve parola ikilisinden oluşan bir meydan okumayla karşılaşır. İstemci, bu meydan okumayı karşılayabildiğinde artık sistemin sağladığı tüm işlemleri gerçekleştirme yetkisine sahip olmaktadır. Tek kullanıcılı veya temel yetkilere sahip bir sistemde bu mekanizma görevini yerine getirmektedir. Ama mekanizma, kullanıcılara farklı yetkilerin atanması veya farklı hizmetlerin kullanılması durumunda yetki denetimi için yetersiz kalmaktadır.
- Bir başka yetki denetim mekanizması olan Kerberos, kimlik denetimi ile yetkilendirme ile kimlik doğrulama mekanizmasında eksik kalan, yetkinin belirli bir süre için verilmesi işlevini, protokole dâhil ettiği zaman bileti vasıtasıyla sağlar. Ama temel kimlik doğrulama mekanizmasına benzer şekilde, yetkilendirme, herhangi bir işlem seviyesinde kısıtlanmamaktadır. Kullanıcı, sisteme dâhil

olduğunda sistem iş akışında bulunan tüm işlemleri gerçekleştirme yetkisine sahip olabilmektedir.

- RADIUS kimlik doğrulama ve yetkilendirme sisteminde ise erişim denetim listeleri kullanılmaktadır. Bu listeler yardımıyla kullanıcılar, temel gruplara yerleştirilmekte ve sistemde bu grupların gerçekleştirebileceği işlemler kapsamında yetki denetimi yapılmaktadır. Erişim denetim listeleri, yetki denetiminin uygulanacağı işlemlerin tanımlanması ve yetki kısıtlamalarının uygulanması açısından yetersiz kalabilmektedir.
- ABAC ve RBAC gibi rol tabanlı erişim denetim mekanizmaları, rollerin işlemler üzerindeki yetkilerinin tanımlanması, yetki devri ve yetkilerin iptali gibi işlevsel özellikleri yerine getirmek için gerçeklenmektedir. Rol tabanlı mekanizmalar, kurumsal yapıda, iş akışında yetki denetimini kurumsal politika, yönetmelik ve kılavuzları içerecek kadar etkin tanımlanmamıştır.

Bu bilgiler ışığında, kurumsal iş akışında uygulanan yetki denetimi mekanizmalarının hedeflenen güvenlik seviyesini yerine getirmeleri için, değerlendirilmeleri, zayıflıklarının giderilerek kurumsal risk toleransına uygun olarak düzenlenmelerine ihtiyaç olduğu görülmektedir. Bu tez çalışmasında, yetki denetiminin her aşamasında yer alan mekanizmalar için bir analiz aracının oluşturulması ve var olan eksikliklerin ortaya konulması ve giderilmesiyle yetki denetiminin devamlılığının sağlanması için bir model sunmaktadır.

Bilindiği gibi, bilgi güvenliği, değerli bilgi varlıklarını yetkisiz erişim, bozma, yok etme ve gizli bilginin açığa çıkması gibi saldırı ve tehditlerden korumak için planlanan ve uygulanan adımların bütünüdür. Bu adımlar, güvenlik mekanizmaları, izleme ve kontrol cihazları, güvenlik yazılımları, yönetmelikler, standartlar, politikalar ve bilgi güvenliği eğitimleri gibi birçok farklı uygulamayı içerebilmektedir. Bir sistemin güvenlik gereksinimleri o sistemde yer alan bilgi varlıklarının önem derecesi ile doğru orantılı olarak artma eğilimindedir. Bilginin değeri ve önemi arttıkça, bilgiyi ele geçirmek için yapılacak saldırı da daha üst düzeyde ve o seviyede karmaşık olabilmektedir. Bu durumda, sağlanan güvenlik seviyesi de detaylı bir gereksinim ve açıklık analizi ile bu analizler doğrultusunda öngörülen veya tespit edilen güvenlik problemlerinin çözümü için uygulanan çözümlerle ilişkilidir.

Süreç daha temel olarak ele alındığında, bilgi sistemlerinde, bilginin okunması, işlenmesi, saklanması gibi işlemlerin bilgiye erişim ile mümkün olduğu görülür. Bir

kullanıcının, bilgi sistemindeki erişim süreci ise sistemde oturum açması ile başlar. Sürecin bu ilk adımında, yetki denetimi mekanizması, erişim isteğinde bulunan kişiye kullanıcı tanımlamasına uygun olarak erişim izni verir. Bu yetkilendirme işlemi kullanıcının tanımlanmasını içeren kimlik doğrulama mekanizması ile gerçekleştirilir. Kimlik doğrulama, bir bilgi varlığına onun özniteliklerinin değerlendirilerek sistem erişim izninin verilmesi olarak tanımlanmaktadır. Bu aşamada yetkili kullanıcılara sistem erişim izni verilirken diğer erişim isteğinde bulunanlar sistem erişim kapsamında reddedilmektedir.

Bir sistem üzerinde uygulanan bir kimlik doğrulama hizmeti, sistem kapsamında kontrol sağlar. Bu genel erişim yetkisi ile birlikte, kimliği doğrulanarak sisteme dâhil olan kullanıcılar için, sistem içerisinde gerçekleştirilecek işlemlerin denetlendiği, kimlik doğrulamanın üzerinde bir yetkilendirme mekanizması gereklidir. Bu mekanizma, iş akışındaki bir sonraki aşamayı, yani sistemdeki kullanıcıların süreçte yetkileri dâhilinde gerçekleştirdikleri işlemleri kapsamalıdır. Bu gereksinimi, kimlik doğrulama ile sisteme dâhil edilen istemcilerin ki bunlar, iş akışında iç kullanıcılar olarak adlandırılabilir, sistemde gerçekleştirebilecekleri işlemlerin etkileri analiz edilerek açıklanabilir.

Geçmiş çalışmalar ortaya koymaktadır ki bilgi sistemlerindeki güvenlik açıkları veya bilgi zafiyetlerinin önemli bir oranı kimliği doğrulanmış ve sistemde tanımlı iç kullanıcılar tarafından gerçekleştirilmiştir. Güvenlik araştırmasına göre [1], 2004'ten 2014 yılına kadar iç kullanıcılar tarafından gerçekleştirilen saldırı oranı %28'dir. 2013'te bu oranın %23 olması iç kullanıcıların sistem açıklarından faydalanarak saldırı eğilimini arttırdığı görüşünü desteklemektedir. Yine aynı araştırmaya göre 2014 yılında, bu saldırılardan oluşan kurumsal zarar, gerçekleşen tüm zarar içerisinde %46 gibi büyük bir meblağı kapsamaktadır [2].

Gerek bilinçli gerekse istem dışı sistem varlıklarına verilen bu zararların temel sebepleri arasında güvenlik mekanizmalarının yetkinlik sınırlarının doğru tanımlanmaması yer almaktadır. Kimlik doğrulama ile sisteme erişim hakkı kazanan ve sistemin iç kullanıcısı olan kişiler, sistem genelinde geniş yetkilere sahip olmaktadır. Sistem genelinde güvenlik zafiyetine sebep olabilecek bu durum, yetki tanımının esnekliğinden dolayı güvenliğin aksamasına ve iş sürecinde kimlik doğrulama ile sağlanan yetkilendirmenin iç kullanıcılar tarafından kötücül amaçlarla kullanılmasına olanak tanımaktadır.

Bu zafiyete örnek olarak verilebilecek bir bilginin açığa çıkması ve veri kaybı vakası 2007 yılında İngiltere'de gerçekleşmiştir [3]. Yetkili bir ofis çalışanı, kendisinden talep edilen, bölge halkına ait birkaç binlik veri içeren kısıtlı bir kaydın çıktısını alarak merkeze iletme görevini, tüm yerleşimci bilgilerini içeren, 25 milyon kayıttan oluşan bir veri tabanını yazılabilir disklere kopyalama ve posta yoluyla merkeze iletme şeklinde gerçekleyebilmiştir. Burada, çalışanın iş süreci bilgisindeki eksikliğinin yanında asıl önemli olan çalışanın veri tabanındaki tüm alanlara erişip bu dışa aktarma işlemini yapabilmesidir. Bu geniş yetki tanımı büyük miktarda kritik verinin açığa çıkmasına yol açmıştır. Disklerin iletim adresine ulaşamadan postanede kaybolması ise gerçekleşen vakanın vahametini pekiştirmektedir.

Kullanıcıların, yetkilendirmenin dikkatli yapılmadığı durumlarda sistemin beklendiği gibi çalışmasına zarar verdikleri de bilinmektedir. Bilinçli olarak yetkilerin kötüye kullanılması veya yetki sınırlarının genişletilmesi bu türden saldırılara örnek olarak sunulabilir. Yukarıda belirtilen anket çalışmasına [1] göre iç tehditlerin %63'ü kurumsal bilgiye yetkisiz erişimden kaynaklanmaktadır.

Kimlik doğrulama mekanizması ile gerçekleştirilen yetki denetimi, yetkisiz erişimleri de önleyecek şekilde yapılandırılmalıdır. Kimlik doğrulama ve erişim tabanlı yetki denetiminin hassas bilgi ve kayıtların güvenliği için yetersiz olduğu bilinmektedir [4]. Örneklenen vakalara benzer şekilde sadece kimlik doğrulama ile sağlanan erişim tabanlı yetki denetim mekanizmalarında kötücül niyetli kullanıcılar, hasta kayıtları veya yukarıda örneklenen yerleşimci bilgileri gibi verilere erişerek kişisel bilgiler gibi hassas verilerin açığa çıkmasına sebep olmaktadırlar [4], [5].

Sunulan örnekler ve veriler ışığında, yetki denetimi mekanizmasının, iş sürecinin oturum açma aşamasının devamındaki süreçlerinde, kimlik doğrulamanın yanında farklı mekanizmaları içermesinin gerekliliği açıktır. Bu mekanizmalar, kimlik doğrulama mekanizmasının sağladığı kimin sisteme giriş, sistemi kullanma izni var kontrolünün yanında kimin belirli bir işlemi gerçekleştirme yetkisi olup olmadığının kararını verebilmeli ve ilgili kontrolü de sağlamalıdır.

Temel oturum açmanın yanında, Kerberos [6] kimlik doğrulama, RADIUS [7] kimlik doğrulama ve erişim denetimi ile rol tabanlı erişim denetimi (RBAC) mekanizmaları görece olarak daha karışık ve farklı yetkilendirme modellerinin uygulandığı yetki denetim mekanizmalarındandır. Bu yöntemler kullanıcıları ve yetkileri, kullanıcı grupları ve roller gibi farklı tanımlar ile belirginleştirerek sistemin doğru ve planlandığı gibi çalışmasını desteklemektedir [8], [9], [10].

Sistemin doğru çalışması, iş süreçlerin planlandığı gibi görevlerini yerine getirmesi kadar bilgi sisteminin ürettiği çıktılardan olan belgelerin doğru ve geçerli olacak şekilde üretilmesi ile ilişkilidir. Bir belgenin doğru ve geçerli olması, belgenin orijinalliği, içindeki bilginin tutarlılığı ve kurum içi ve kurumlar arası kapsamlarda belgenin kabul görmesine bağlıdır. Bu belge, kurumsal iş akışında planlanan ve geçerli süreçlerde, kurumsal politika ve yönergelere uygun olarak üretilmiş olmalıdır. Belgenin kabulü, belgenin sadece yetkili şahıs ve kabul gören süreç içinde üretildiğinin ispatı veya bu ispat bilgisinin varlığı ile mümkündür. Eğer bir belge kurum dışına çıkacaksa geçerliliğini kurum dışında da sürdürebilmeli, doğruluğuna dair ispat verisini kurumsal iş süreci dışına çıktığında da koruyabilmelidir. Bu durumda bilgi sistemi belge için hem kurum içinde hem de kurum dışında doğrulanabilir olma yeteneğine sahip olmalıdır.

Bu bağlamda, bilgi sisteminde, bir belgenin orijinalliği, belgenin yetkisiz olarak değiştirilmediğini, düzenlenmediğini ispatlayan bir yöntemin varlığıyla desteklenebilir. Bilindiği gibi, belgeyi oluşturan kişi bilgisinin daha sonra doğrulanabilir olmak üzere belgeye eklenmesi sayısal imzalar ile mümkün kılınmaktadır. Bu işlemde, belgeyi oluşturan veya işleyenin kimliğine olan güven kriptografik yöntemlerle sağlanmaktadır [11].

Hem bilgi sisteminin hem de bu sistemde üretilen, işlenen belgenin doğruluğu ve güvenilirliği için sistemde yer alan ve örnekleri yukarıda verilen bu mekanizmaların yetkinliklerinin incelenmesi elzemdir.

İş akış süreçlerinde güvenlik yönetimi, güvenlik kurallarının uygulanmasından oluşur. Bu kurallar, kurumsal güvenlik politikalarında tanımlanmaktadır. Temel kurumsal yönergeler, devletin belirlediği yönetmelikler, güvenlik standartları ve hatta kurumlar arası güvenlik sözleşmeleri bu politikaların kapsamını oluşturur. Bunlarla birlikte güvenlik politikaları genel olarak iş akışında yer alan işlemler ve kurumdaki roller üzerinde tanımlı kısıtlamaları tanımlar [12].

Bir iş akışı, bir kurumda bir veya daha fazla birimin dâhil olabildiği süreçlerden oluşur. İş akışı aynı zamanda kurumlar arası yazışmalarda olduğu gibi farklı kurumların da katıldığı süreçleri içerebilir. Güvenlik politikalarının iş akışına uygulanması sırasında bu çeşitlilikten kaynaklanan sorunlar çıkabilmektedir. Bu sorunlar, temel olarak, farklı birim veya kurumlarda uygulanan değişken kısıtlamaların oluşturduğu tutarsızlıklardan kaynaklanmaktadır [12].

Süreğen yetki denetimine ait destek belgesinde [13] yetki denetiminin üç

aşamasından biri yeniden yetkilendirme olarak tanımlanmaktadır. Bu aşamada, yetki riski yeniden değerlendirilir veya yetki mekanizması kontrol edilir. Bilgi sisteminde, ilk aşama olan yetki denetiminin oluşturulması ve süreğen yetki kontrolü adımlarından sonra bakım veya işlem aşamalarında mekanizmayı gözden geçirmeyi önerilmektedir. Bu gözden geçirme, risk değerlendirmesi ve kurumsal risk toleransı kapsamında yeniden yetkilendirmeyi tetikler. Yeniden yetkilendirme, kapsam olarak, donanımsal portların değiştirilmesi gibi küçük işlemleri içerebildiği gibi güvenlik mekanizmaları ve yönergelerinin değiştirilmesi gibi köklü yapılandırmaların da gerçekleşebildiği bir süreçtir.

Kurum içi ve kurumlar arası yazışma belgelerinde, kurumsal yetkilerin kullanılabilmesi, belgenin özgünlüğünün belirlenebilmesi ve doğrulanabilmesi işlevselliği, Bilgi ve Belge Yönetim Sistemi (BBYS)'nin bütünlüğü için önemlidir. Benzer biçimde, bu belgelerin uzun süre arşivlenmesinde belgenin sahip olduğu doğrulanabilir özgünlüğünden bir şey kaybetmemesi gerekmektedir.

E-imza ile bütünlüğü ve kimin işlemi gerçekleştirdiği bilinen bir belge, BBYS içerisinde doğrulandığında işlemi gerçekleştirenin yetkileri onaylanabilmektedir. Arşivlenmiş belgede ise zamanla değişime uğrayan belgelerde, bu işlem günlük ve geçmiş bilgileri ile dolaylı olarak gerçekleştirilmektedir. Kurumlar arası yazışmalarda ise yetkinin taşınması söz konusu olmamaktadır. Yetki, sadece belge üzerinde iddia edilen ve doğrudan geçerliliğinin sorgulanması mümkün olmayan bir yapıdadır.

1998 yılında başlayıp 5 yıllık raporlama dönemleriyle devam eden ve bu çalışmanın yapıldığı zaman, dönemi 2013-2018'i kapsayan uluslararası elektronik sistemlerdeki kalıcı otantik belgelere ilişkin araştırma projesi olan InterPARES [14] projesi BBYS'nin kullanımı açısından önemli bir araştırma olmuştur. Bu proje, belgelerin uzun süre saklanması, iş sürecinde kayıtların oluşturulmasından yok edilmesine kadar olan statik ve dinamik işlemleri, kurumların yaklaşımlarını, güvenlik, kontrol ve altyapı mekanizmalarını hedefleyen çalışmalar yapmaktadır. 2012 yılında yayınlanan [15] "Türkiye'de Kurumsal Elektronik Bilgi ve Belge Yönetimi Uygulamalarına Dönük Koşulların Değerlendirilmesi: 57 Örnek Kurumun Analizi" çalışmasının verileri temel alınarak var olan uygulamalar değerlendirilmiştir.

Adı geçen çalışmada, "bilgi içeriğinin üretimi, düzenlenmesi ve dosyalanması, saklama koşullarının tanımlanması, korunması ve güvenliği ile kayba uğramadan uzun süre saklanmasına dönük koşulların ve beklentileri analizi" yapılmış ve var olan durum ile beklenti ve gereksinimlerin tespitine yönelik kurumlar düzeyinde bir analiz

gerçekleştirilmiştir. Çalışma, kamu, özel sektör, üniversite ve sivil toplum kuruluşlarını kapsayan 57 Kurum üzerinde idari ve teknik personellerle uzman ve yöneticilerin katılımıyla sağlanmıştır.

Bu çalışmada, e-imza kullanılan gruba göre yapılan araştırma sonuçlarından elde edilen bazı bilgiler Tablo 1.1'de sunulmaktadır.

Tablo 1.1: Kurumlarda Elektronik İmza ile İlgili Uygulama İstatistikleri

Dokümanlarda E-imza Kullanım durumu:	%11,8 kullanıyor %19,8 uygulama yürütülüyor ama kullanmıyor
E-İmza Kullanım alanları:	Kurum içi tüm yazışma ve talimatlar %44,5 Bazı haberleşme ve iletişim işlemleri %54,3 Diğer kurumlarla yazışmalar %1,2
Elektronik Bilgi ve Belge Yönetim Sistemi (EBBYS) Kullanımı	Hiç %2,8 (Bütünüyle-İleri-Orta-Yüzeysel) %97,2
Kurumlarda EBBYS yönelik yaşanan kaygılar	%37,2 özgünlük, %12,6 yetkilendirmeler, %15,8 uzun süre koruma, %7,3 belge bütünlüğü

Anket sonuçlarından, E-devlet sürecinde, kurumlar arası yazışmalarda e-imzanın (elektronik belgenin güvenli taşınması) gerektiği gibi varlığını göstermediği görülmektedir. Oysa bu kurumların büyük çoğunluğunun Elektronik BBYS'ye sahip olduğu gözlemlenmiştir.

Raporun sonuçlarında, "Yasal ve idari koşulların uyumluluğuna dönük oluşturulan düzenlemeler ve gelişen teknolojik koşullara karşın, kurumların EBBY uygulamalarına dönük temel kaygısı olan güvenilirlik ağırlıklı olarak yerini korumaktadır. Bilginin özgünlüğü, yetkilendirme ve uzun süre koruma ile ilgili kaygılar güvenilirliğin gölgesinde kalmaktadır. Genel olarak EBBY uygulamalarına dönük kaygı duymayanların oranı %10'un altında kalmaktadır. Bu sonuç var olan sistem alt yapısının geliştirilmesine ve kullanılan sistemlere güven sağlamaya dönük bilgilendirici faaliyetlere daha fazla zaman ayrılması gerektiğini göstermektedir." çıkarımları yer almaktadır.

Tablo 1.1'in son maddesi ise tez çalışmasının kurumların sahip olduğu kaygıların küçümsenmeyecek bir kısmını hedeflediği görülmektedir. %68,4'lük

güvenlik kaygılarının buna dâhil edilmediği bilinmelidir.

Kurumların, elektronik ortama öncelikli geçiş talep ettikleri işlemler arasında kurumsal iletişim ve yazışmalar ile arşiv işlemleri için sırasıyla %66,1 ve %44,8 oranda ortak görüş belirtilmiştir.

2014 yılında yayımlanan bir diğer çalışma [16], Kalkınma Bakanlığı örneğinde, arşiv ve belge yönetim sisteminde (AVBYS) karşılaşılan sorunların analizini yapmış ve çözüm önerileri sunmuştur. Çalışma, sistem üzerinde belgelerin tanımlanması, erişim yetkilendirmeleri ve sınırlamaların yetersizliği konusundaki sorunların varlığının vurgulamaktadır. Sonuç önerilerinde tanım alanları ile ilgili iyileştirmelerin yapılması, kurumsal işlemlerin kanıtı niteliğindeki belgelerin yönetiminin etkin bir biçimde gerçekleştirilebilmesi ve kurumsal hafızanın korunmasının önemi vurgulanmaktadır. Geliştirilecek çözümler ile sistemlerin iyileştirilmesi elektronik belge yönetiminin sürdürülebilirliği açısından önemli görülmektedir.

1.1. Tezin Amacı, Katkısı ve İçeriği

Kerberos'un dağıtık sistemlerde yetkilendirme konusundaki eksiklikleri ve güvenlik için yetkilendirme mekanizmasına ihtiyaç duyduğu bilinmektedir [8]. Tez çalışmasında yapılan erişilebilirlik analizi, sadece kimlik denetiminin iç saldırganın yetkisiz belge üretebilmesinin önüne geçemediğini ortaya koymakta ve desteklemektedir. Erişim denetim listeleri, kullanıcı ve işlemler için sahip oldukları kısıtlı tanım aralıklarından dolayı, iş akışında karmaşıklaşan işlemler söz konusu olduğunda yetersiz hale gelmektedir [9]. Bilindiği gibi, rol tabanlı erişim denetimi yöntemleri [8], [10] erişim denetim listelerinin yetersizliklerine [9] çözüm olarak önerilmiştir. Kullanıcıların genel tanımlarla yapılmış yetki kısıtlamalarını iş akışında atlatarak yetkisiz belge üretimi/onayı yapabildiği yine gerçekleştirilen erişilebilirlik analizi ile sunulmuştur.

Sayısal imzalar tasarlanırken belgenin özgünlüğünün korunması ve kimlik doğrulama fonksiyonları ön planda tutulmuş ama bu politika ve yönergeler imzaya ait iç parametreler olarak imza şemalarında şimdiye kadar yer bulamamıştır. İlgili çalışmalarda örnekleri sunulan vekil [17], grup [18], [19] ve kimlik tabanlı [20], [21] imza şemalarında, kişisel imza yetkilendirmelerinin düzenlenmesi söz konusuyken; kurumsal yetkinin kullanımı ve kurumsal yetkilerin imza ile denetlenebilmesi

hedeflenmemektedir. Söz konusu çalışmalarda, imza ile ilişkilendirilen bilgi, çalışmayla sunulan şemada, imzaya eklenen kurumsal imza yetkilerini içermemektedir. Belirtilen eksikliklere çözüm getiren çalışma, bu bakımdan özgün niteliktedir.

Bu çalışmada, kurumsal iş akışındaki belgelerde, yetki denetiminin, kurumlar arası ve arşiv gibi süreç dışındaki sürdürülebilirlik problemi sunulmuş ve problemin Petri ağları yöntemi ile yapılan analizinde, kurumsal iş akışında yetki denetiminin eksiklikleri değerlendirilmiştir. Vaka çalışması olarak, kurumsal uygulamalarda, yetki politikalarına ve imza yetkisi yönergelerine tabi olan onay belgeleri üzerinde yetki denetimi ele alınmıştır. Önerilen model, gerçeklenerek güvenlik ve performans analizleri yapılmış ve pratikte kullanılabilirliği tartışılmıştır. Sunulan modelin bütünsel yapısında yer alan yetkilendirme makamı için farklı mimariler önerilerek modelin uyumluluğu artırılmıştır.

Çok katmanlı yetki modeli, temelde yetki denetim yöntemlerini, yetki denetim sürecindeki yetkinliklerini ve farklı mekanizmaların birbirleri arasındaki ilişkiyi ortaya çıkararak, analizlerini gerçekleştirmek üzere sunulmuştur. Modelde, kurumsal yönergelerin ele alınmamasından kaynaklanan yetki denetim problemlerine çözüm olarak, dördüncü katman olarak yeni bir yetki denetim mekanizması da sunulmuştur.

Model, kurumsal iş akışında yetki denetim uygulayıcıları için temel bir rehber olma niteliğindedir. Uygulayıcılar, katmanların yeteneklerini göz önünde bulundurarak gereksinimlerine göre, sistemlerinde mekanizmaları yapılandırabileceklerdir. Karar vericiler, modeldeki katmanların kapsam ve işlevsel sınırlarına göre gerekli gördükleri yetki denetim mekanizmalarına karar verebileceklerdir. Model, uygulayıcıların kendi sistemlerini analiz edebilecekleri sistem iş akışı için bir şablon sunmaktadır. Uygulayıcılar, analiz sonucunda gereksinimlerini karşılamadığı düşünülen uygulamalar için sistemlerinde bir üst katmanda yer alan yetki denetim mekanizmasını gerçekleyerek iyileştirme yoluna gidebileceklerdir.

Önerilen model, tek kullanıcılı, kullanıcının tüm yetkiye sahip olduğu sistemler için kullanışlı değildir. Bu ve benzeri sistemler, kullanıcıya ya tüm erişim haklarının verildiği ya da tüm erişimlerin reddedildiği tek bir katmandan oluşurlar. Mobil istemciler veya dağıtık sistemler için, model, ilk analiz adımında kullanılarak yetki denetim gereksinimi veya ihtiyaç duyulan mekanizmanın çıkarılması için kullanılabilir.

Model, yetki denetiminin yüksek önem arz ettiği kurumsal iş akışlarını temel

almaktadır. Çoğu sistemde, yönetmeliklerde tanımlanan kurumsal yetkiler, yetki denetiminde karşılık bulmamaktadır. Model ile bu yetki denetim zafiyetini ortaya konularak, önerilen üst katman ile bir çözüm önerisi sunulmaktadır. Model, yetki denetim yapılandırmasının nihai halini aldığını öne sürmediği halde özel yetki denetim gereksinimlerine ihtiyaç duyan uygulamalar için modelin üstünde başka bir katmanın konulmasını önlemeyecek şekilde yapılandırılmıştır. Çok katmanlı model, var olan çok yetkili sistemlerdeki yetki denetim mekanizmalarının incelenmesi için bir rehber olabilecektir. Bu gözden geçirme, yetki denetim kapsamının güncellenmesi ve var olan katmandan bir üst katmana geçişi tetikleyebilir. Önerilen model, var olan sistemin analizi ve fark edilmeyen kritik zafiyetlerin ortaya çıkarılması için kullanılabilecek yetenektedir.

2. ÖN BİLGİ VE LİTERATÜR ANALİZİ

Bu bölümde, çok katmanlı yetki denetim modelinde yer alan yetki denetim mekanizmalarına ait bilgiler sunulmakta, mekanizmaların yetenekleri kısaca özetlenmektedir. Modelin dışında tutulan mekanizmalara yine bu bölümde değinilmiştir.

2.1. Kerberos

Kerberos, açık ağlarda kimlik doğrulama için tasarlanmış, gizli anahtar tabanlı bir hizmet protokolüdür. Kimlik doğrulama, anahtar dağıtım merkezi (KDC) olarak adlandırılan güvenilir bir üçüncü taraf ile desteklenmektedir.

Her kullanıcı, KDC ile bir gizli anahtar paylaşır. KDC, kullanıcılara ve hizmet almak istediği sunucuya zaman kısıtlı bir oturum anahtarı iletir. Kullanıcı, yani istemci, sunucu ile paylaştığı bu anahtarla, ilgili oturum boyunca işlem gerçekleştirebilecek yetkiyi almış olur.

Kerberos v5 ile istemciler, ilk olarak, kimlik doğrulama birimine kendi kimliklerini kanıtlamak zorunda bırakılmaktadır. Bu işlem, aradaki adamın kullanıcının önceki mesajlarını kullanarak sunucu için oturum bilgisi elde etmesini önlemeye yöneliktir. Kullanıcıya, üretilen bir zaman pulu, kendi anahtarıyla şifrelenmiş olarak gönderilir. Eğer, kullanıcı, iddia ettiği kişi ise bu şifreyi çözerek cevabı gönderebilecektir. Zaman pulu, burada, çevrimdışı saldırılara da bir önlem olarak kullanılmaktadır. Kerberos kendi alanı dışındaki sunucular için bir oturum anahtarı oluşturamamakta ve işlemlere erişim izni vermemektedir. Bu da, kullanıcıların sistem dışında farklı Kerberos sunucularına erişim istekleri için başka başka kimlik doğrulama ve yetkilendirme sunucularından hizmet alma gerekliliğini ortaya çıkarır. Eğer, bu sunucular, birlikte çalışmıyorlarsa her sunucu ile her kullanıcının anahtar paylaşmasını gerektirir.

Kerberos altyapısı, kullanıcılar için kimlik doğrulama ve sunucular için oturum temelli yetkilendirme işlevini gerçekler. Ama işlemsel yetkiler için bu altyapı yeterli olmamaktadır. Sistem, sunuculara, oturum temelli erişim ve işlem gerçekleştirme yetkisi verir ve oturum sona erdiğinde atanan yetki sonlanmış olur. Kerberosta yetkinin devri söz konusu olsa bile toplu işlemlerin gerçekleştirilmesinde oturum süresi kısıtı

sorun oluşturmaktadır. Bununla beraber erişim yetkilerinin farklı sunucular arasında paylaşılmış olması gereklidir. Bu da, gizli anahtar temelli doğrulama mekanizmasından dolayı, anahtar paylaşım ve yönetiminde yük getirmektedir.

Daha üst seviye yetki denetimi ve sistem genelinde erişim yetkisi yerine işlemsel yetkiler için daha gelişmiş yetki denetim mekanizmaları geliştirilmiştir. Rol tabanlı erişim denetim mekanizması da bunlardan biridir.

2.2. RBAC(Role Based Access Control)

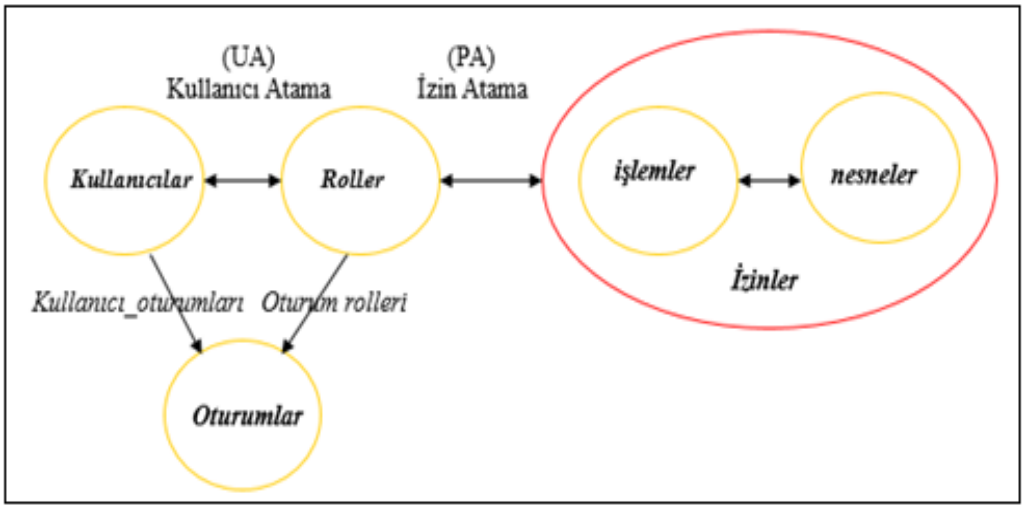
Ağ sistemleri ve karmaşık iş akışları geliştirilmeden önce, kullanıcıların, sisteme veya sistemdeki birim ve belgelere erişimi oturumlar tarafından sağlanıyordu. Bu sistemde, kullanıcılar, sisteme kimliklerini doğrulayarak giriş yapar ve kendileri için oturum olarak belirlenen sınırlı bir zaman aralığında sistemde yer alırlar. Oturum bazlı yetkilendirme olarak adlandırılan bu mekanizmada kullanıcılar için belirli gruplar tanımlanır. Bu gruplar farklı tipteki kullanıcılar için değişik seviyelerde izinlerin tanımlanmasına olanak sağlar. Kullanıcının yetkilendirilme işi bu izinlerle sağlansa da bu yaklaşım, karmaşık yetkilendirme gereksinimlerini karşılayamayıp kısıtlı bir yapı sunabilmektedir [22]. Bir kullanıcıyı birden fazla farklı grup içinde tanımlamadan değişik yetkilerin kullanıcı için atanması mümkün olmamaktadır.

1997 yılında Ferraiolo ve diğerleri kimlik doğrulama ve erişim denetimi için rol tabanlı erişim denetimi (Role Based Access Control, RBAC) modelini sunmuşlardır [10]. Bu modelde, izinler, kullanıcılarla ilişkilendirilmek yerine rollerle ilişkilendirilmiş ve kullanıcıların bu rollerle ilişkileri kurularak yetki denetimi mekanizması sağlanmıştır.

RBAC, beş farklı temel elementi içerir [23]. Bunlar; kullanıcılar, roller, işlemler, izinler ve nesnelerdir. Kullanıcılar, bir nesneye kendilerine atanan rol ile erişebilirler. Roller ise gerçekleştirilen görevler üzerine kurulmaktadır. Bu kapsamda tanımlanması gereken bir diğer kavram da izin olmaktadır. İzinler, bir işin veya görevin gerektirdiği yetki ve sorumluluğu içerir. Bir nesne üzerindeki işlemler, tanımlı izinler ile gerçekleştirilebilir. Son olarak nesne, kullanıcı yerine kullanıcının rolü ile ilişkilendirilmiş olur. Roller, kullanıcılara, kullanıcı atama (user assignment) ilişkisi ile atanır. İzinler ise rollere benzer şekilde izin atama (permission assignment) ilişkisi ile atanır.

Roller, en az izin kuralına göre inşa edilir. Bu kural, bir nesnenin erişilebilirliği için mümkün olan en az izni içerecek şekilde tasarlanmasını hedefler. Bir kullanıcı, sadece kendisinin gerçekleştirmesine izin verilen bir role atanır ve o rolün gerektirdiği işi gerçekleştirir. Hiçbir rol bir kullanıcıya aynı rolün başka bir kullanıcı için tanıdığı izinlerden fazlasını veremez.

Temel RBAC yapısı ve geliştirilen 4 farklı RBAC modelinin hiyerarşi ve kısıtlara uygunluğu sırasıyla Şekil 2.1 ve Tablo 2.1'de sunulmaktadır.



Şekil 2.1: Temel RBAC yapısı

Tablo 2.1: RBAC Modellerinin Özellikleri

Modeller	Hiyerarşi	Kısıtlar
$RBAC_0$	Yok	Yok
$RBAC_1$	Var	Yok
$RBAC_2$	Yok	Var
$RBAC_3$	Var	Var

RBAC modeli farklı güvenlik politikalarının tanımlanabilmesine olanak sağlayarak oturum tabanlı sistemden daha kolay bir güvenlik yönetimini destekler. Bununla beraber, sistem, rol tanımlamalarının sabit olmasından dolayı, esnek kuralların tanımlanması ve karışık güvenlik politikalarının uygulanabilirliği konusunda hâlâ yetersizlik göstermektedir [22].

2.3. Sayısal İmza

Tez çalışmasındaki hedeflenen çalışmalardan biri de kurumsal belgelerde yetki denetimini destekleyen, kimin hangi işlemi onayladığı, belgenin orijinalliği ve bütünlüğü gibi bilgileri oluşturulan sayısal belge kapsamında doğrulamaya yarayan sayısal imza mekanizmasının iyileştirilmesidir.

Sayısal imza, sayısal bir veriye eklenen ya da o sayısal veriyle mantıksal bağlantısı olan, kimlik doğrulama amacıyla kullanılan başka bir sayısal veri olarak tanımlanmaktadır[23].

Sayısal imza aynı zamanda, güvenli bir imza oluşturma aracı ile oluşturulma, nitelikli bir sayısal sertifika ile imza sahibinin kimliğinin tespitini ve imzalanmış sayısal veride imza sonrası herhangi bir değişikliğin yapılıp yapılmadığını sağlayabilme yeteneğine sahip olmalıdır[24].

Sayısal imza şeması kavramı, Diffie ve Hellman tarafından 1976'da ortaya konulmuştur[25]. 1978'de Rivest, Shamir ve Adleman, günümüzde yaygın olarak kullanılan sayısal imzalama algoritmasının temellerini atmıştır[26]. Sonraki yıllarda, gelişen kriptografik yöntemler ile ElGamal, ECDSA gibi birçok sayısal imzalama şeması literatürde yerini almıştır[27].

Sayısal imzalama, imzalanacak belgenin tek yönlü bir özetleme fonksiyonu ile özgün bir özetinin elde edilmesi ve bu özetin belirlenen imzalama algoritmasından geçirilmesi aşamalarından oluşan işlemdir. Bu işlemin sonucunda o belgeye ait bir sayısal imza elde edilmiş olur.

Sayısal imzanın doğrulanması ise; belgenin aynı özetleme fonksiyonu kullanılarak özetinin oluşturulması ve bu özetin imzalayan kişiye özgü bir anahtar/sertifika ile çözümlenmiş özetle karşılaştırılması aşamalarını içerir. Anahtar kullanımı, kimliğin doğrulanmasını, özetlerin karşılaştırılması ise belgenin bütünlüğünün doğrulanmasını sağlar.

Sayısal imza mekanizmalarının işlevsel hedeflerini uygulamalarda gerçekleştiremediği durumlar da mevcuttur. Örneğin, imzada kullanılan özetleme bilgisinin güvenilirliğinin ortadan kalkması imzanın tamamının geçersizliği gibi beklenmeyen bir durum ortaya çıkarabilmektedir. Söz konusu bu zayıflık uzun süreli arşivlenen belgelerin güvenilirliğinin sağlanmasında sorunlar ve çözümde yeni yaklaşımlar ortaya çıkarmaktadır. Benzer şekilde, kişi bilgisi kaynaklı imzalar ile

belgenin orijinalliği veya belgeyi oluşturan kişi doğrulanabilirken bu kişinin imza kullanılarak işlem yetkisi doğrulanamamaktadır.

Kerberos bölümünde örneklendiği gibi kurumsal güvenlik uygulamalarının kurum dışına çıkarılması farklı kurumlarda yetkilerin denetiminde zorluklar getirmektedir. İşlemlerin, kurum içinde yetki denetimi iş akışı ile kontrol altına alınırken kurumlar arası yazışmalarda iş akışı farklılaşmakta ve kurumsal yetkiler soyutlaşmaktadır. Tez çalışmasında, sayısal imzalı belgelerin kurumlar arası yazışmalarda yetki denetiminin sürdürülebilirliğine katkıda bulunması hedeflenmiştir.

Tez çalışmasında, yetki denetim mekanizmalarının iş akışında yetkinliğinin kontrolü için Petri ağlarından faydalanılmıştır. Petri ağları hakkında takip eden bölümde bilgi verilmektedir.

2.4. Petri Ağları

Petri ağları, lineer cebir ve benzeri matematiksel modelleri kullanarak iş akışı gibi birçok sistemin modellenmesinde kullanılabilen, sistem davranışının analiz edilebildiği bir araçtır [28].

Petri ağları, matematiksel olarak bir sistemi modellemesinin yanında grafiksel olarak da sistemdeki ilişkileri, sistemin genel yapı ve işleyişini ortaya koyar[29]. Bunun yanında, Petri ağları, matematiksel olarak da durum denklemleri ve ilişkisel matrisler ile sistem davranışının ifade edilmesine olanak sağlar. Bu ifadeler, sistem modelinin bilgisayar yardımıyla işlenmesi ve benzetimlerin oluşturulabilmesini destekler. Bu yönleriyle, bir sistemin tasarlanması, incelenmesi, analizi ve varsa sistemdeki sorunların giderilmesi konusunda Petri ağlarının kullanımından faydalanılmaktadır.

1962'de Carl A. Petri'nin önerdiği bu yapı, iki parçalı yönlü çizgelerin, yer veya durum, olay veya geçiş olarak adlandırılan ve bu ikisi arasındaki ilişkiyi tanımlayan yönlü bir doğrudan (yaydan) oluşan üç tip nesneden oluşmaktadır. Bir yer işaretinin girdi sayılabilmesi için bu yerden bir geçişe yay olmalıdır. Benzer şekilde yer işaretinin çıktı olması için bu yere herhangi bir geçişten gelen bir yay bulunmalıdır.

Bir Petri ağı, iş akışındaki durum ve olay kümeleri ile bu iki küme arasındaki ilişkiyi gösteren bir çizgedir. Petri ağı $\sum$, aşağıda tanımlanmıştır.

- $\sum = \{P, T, F, I, O, M\}$ beşlisi ile tanımlanmak üzere,
- $\mathrm{P} = \{\mathrm{P0}, \mathrm{P1}, \ldots, \mathrm{PN}\}$ sonlu yer kümesi (durum),
- $\mathrm{T} = \{\mathrm{T0}, \mathrm{T1}, \ldots, \mathrm{TN}\}$ sonlu geçiş kümesi (olay) öyle ki $\mathrm{P} \cap \mathrm{T} = \emptyset$
- F sonlu yönlü yay kümesi olmak üzere $\mathrm{F} \subseteq (\mathrm{P} \times \mathrm{T}) \cup (\mathrm{T} \times \mathrm{P})$
- öyle ki $(\forall \mathrm{t} \in \mathrm{T})(\exists \mathrm{p}; \mathrm{q} \in \mathrm{P})(\mathrm{p}; \mathrm{t}); (\mathrm{t}; \mathrm{q}) \in \mathrm{F}.$
- Girdi fonksiyonu $I: (\mathrm{TXP}) \rightarrow \{0,1\}$
- Çıktı fonksiyonu $O: (\mathrm{PXT}) \rightarrow \{0,1\}$ şeklindedir.

Bir Petri ağına ait işaret kümesi M aşağıda tanımlanmıştır:

- $\mathrm{M} = \{M_0, M_1, \ldots, M_n\}$ öyle ki
- M_0 ilk işaret ve $\mathrm{M} \neq \emptyset$ ve $\mathrm{M} \subseteq$ P'dır.

Petri ağları, literatürde, sonlanma, erişilebilirlik, sınırlılık, canlılık, kapsama ve kalıcılık gibi birçok yapısal ve davranışsal özelliklere sahiptir. Tez çalışmasında, Petri ağlarının erişilebilirliği kullanılmaktadır. Erişilebilirlik anlatılmadan önce bir Petri ağının nasıl ifade edildiği ve tetikleme kavramının açıklanması gereklidir.

Tetikleme işlemi, işaret taşıyan (aktif) bir geçişin bir duruma etki edecek şekilde yönlendirilmesidir.

Eğer, bir t_1 geçişi M_0 işaretinden M_1 e tetiklenirse, bu durum $M_0 \xrightarrow{t_1} M_1$ veya $M_0\,[t_1 > M_1$ olarak gösterilir. σ sonlu bir geçiş sırası olmak üzere $\sigma = t_0\, t_1\, t_2\, \ldots t_{n-1}$, bir sonlu tetikleme sırası olarak adlandırılır. M_0 ile başlayan bir sıra $M_1 M_2 .. M_n$ işaretlerinin varlığında $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_2} .. \xrightarrow{t_{n-1}} M_n$ ile gösterilir ve bu gösterim $M_0 \xrightarrow{\sigma} M_n$ veya $M_0\,[\sigma > M_n$ ile özetlenir. Tutarlılık için tez içinde $\xrightarrow{\sigma}$ gösterimi kullanılmıştır.

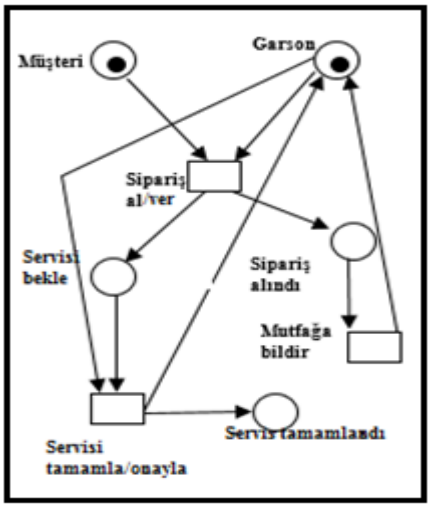
Bir M_n işareti, eğer M_0'dan M_n'ye bir tetikleme sırası bulunuyorsa M_0'dan erişilebilirdir denilir. Erişilebilirlik $M_0 \xrightarrow{*} M_n$ ile gösterilir.

Bir Petri ağının davranışı, genel olarak, o ağın oluşturduğu çakışıklık matrisinin analizi ile gerçekleştirilir. $\sum$ Petri ağı, eğer n geçiş ve m yer içeriyorsa, çakışıklık matrisi $\mathrm{I} = [\mathrm{m_{ij}}]$ den oluşan nXm boyutunda bir tamsayı matrisidir. I ise $\mathrm{I} = \mathrm{I}^{+} - \mathrm{I}^{-}$, yani i geçişinden j yerine olan çıktının büyüklüğü ile j yerine i geçişinden olan girdinin büyüklük farklarından oluşur. Erişilebilirlik bu matriste , $M = M_0 + \mu I$ formülü ile

bulunur. Burada μ , tetiklenebilir yer matrisini ifade eder.

Örnek olarak, Şekil 2.2'de bir garsonun yemek servisi yapması, Petri ağları ile modellenmiştir. Bu modelde garsonun siparişi alabilmesi için müşterinin tetiklenmesi gerekliliği müşterinin işaretlenmesi ile sağlanmıştır. Sipariş al durumunun gerçekleşmesi için garsonun da tetiklenmesi gerekir. Bu, birden fazla garsonun varlığında siparişi alacak garsonun belirlenmesi için önemlidir. Daha sonra sistemin akış ve tamamlanma durumları modelde tanımlanmıştır. Bu senaryo üzerinde, garsonun mutfağa veya müşteriye erişebilirliği olmadığı durumlarda, müşteri tetiklendiğinde siparişin alınması ve sistem akışının tamamlanmasının mümkün olmadığı gözlemlenebilmektedir.

Bu modelde tetikleme işleminin [0,1] ile tanımlanması, müşterinin sipariş vermemesini içerir. Garsonun, müşteri siparişine göre, siparişin tamamlanması erişebilirliği ise, [1,1,0] başlangıç matrisi ve Tablo 2.2'de verilen çakışıklık matrislerine göre [0,1,1] =[1,1,0]+[1,2,1,1,1].I olacaktır. Bu durum, tüm işlemlerin gerçekleştirilmiş olması sonucu gerçekleşebileceğini gösterir. Olası aksi, örneğin mutfağa erişimin olmadığı durumda [1,1,1,1,1] mutfaktan geri dönüş için gerekli tetiklemenin olmadığı durumda [1,0,1] yani t_1, mutfağa bildir, erişilememektedir.



Şekil 2.2: Yemek servisi Petri ağ modeli

Bu çalışmada, Petri ağları, iş akışında yetki denetiminin modellenmesi için kullanılmakta ve iş akışındaki yetki denetim analizi bu ağ üzerinde erişilebilirlik analizi ile gerçekleştirilmektedir.

Tablo 2.2: Çakışıklık matrisleri

	T0	T1	T2
P0	0	1	1
P1	0	0	0
P2	1	0	0
P3	1	0	0
P4	0	0	1

İleri çakışıklık matrisi I^+

	T0	T1	T2
P0	1	0	0
P1	1	0	0
P2	0	1	0
P3	0	0	1
P4	0	0	0

Geri çakışıklık matrisi I^-

	T0	T1	T2
P0	-1	1	1
P1	-1	0	0
P2	1	-1	0
P3	1	0	-1
P4	0	0	1

Birleşik çakışıklık matrisi I

2.5. Durum Analizi

Yetki denetimi, kullanıcının sistem üzerindeki haklarını tanımlayarak sistem üzerinde gerçekleştirdiği işlemleri, bu izinler çerçevesi içinde tutan bir güvenlik mekanizmasıdır. Kurumsal sistemlerde, kullanıcılar, iş akışına dâhil olurken karşılarına çıkan ilk yetki kontrolü, sistem erişimini sağlayan kimlik denetimi tabanlı oturum açma mekanizmasıdır. Çoğu bilgi sistemi, güvenli web servisleri, iş istasyonları, sunucular, ağ cihazları, veri tabanları gibi yapılarda sistem erişim izni, kullanıcıya oturum açma yoluyla verilir. Bu işlem, kullanıcının sisteme erişim isteği göndermesi, sistemin bu isteği, genelde parola sorma gibi bir meydan okuma ile çözümleyip sonuç olarak onay veya ret cevabı vermesi aşamalarından oluşur. İstekte bulunan kullanıcı, kimliğini ibraz etmek ve bu kimliğe bağlı gizli bir bilgiyi kullanarak kendinin iddia ettiği kişi olduğunu kanıtlamak zorundadır. Basit oturum açma, Kerberos [6] ve RADIUS [7] gibi birçok uygulama kimlik denetimini yetkilendirmede kullanır. Basit oturum açma yönteminde, kişi kimliği ve parola birleşimi kullanıcıdan talep edilir. Kerberos'ta ise kullanıcının kimlik doğrulaması çoklu sunucu mimarisi ile gerçekleştirilir. Kullanıcıya, sunucuya belirli bir süre aralığında erişim imkânı sağlayan bir oturum bileti sağlanır. Kullanıcı bu durumda sunucuya kimliği, parolası ve bu bilet ile istekte bulunur.

Fakat sistem bazında erişim iznini kimlik denetimiyle sağlayan bu tip uygulamalar, bazı durumlarda yetkilendirme problemleriyle karşılaşabilmektedir. Kerberos kimlik doğrulama ile erişim denetimi, dağıtık sistemlerde yetki denetiminde zayıflık gösterir. Sistem genelinde erişim yerine kullanıcıların yetkilerinin

tanımlanmasına ihtiyaç duyulmaktadır. Kerberos, kimlik doğrulama tabanlı bir yetki denetimi olarak, gereksinim duyulan güvenlik seviyesi için ek mekanizmaların uygulanmasını ve erişim bileti gibi ek bilgilerin sunulmasını gerektirmektedir [8].

Bir diğer yaygın kimlik doğrulama ve yetki denetimi yöntemi RADIUS'tur. Bu mekanizmada, sisteme erişim izni kimlik doğrulama ile verilir ve yetkilendirme için erişim denetim listeleri kullanılır [7]. Erişim denetim listeleri [9], kimlik denetimine ek olarak, kullanıcılar için sistemde tanımlı belirli işlemlere onay veya ret girdilerini tutan en temel yetki denetimi uygulamalarındandır. Listeler, sistemde tanımlı işlemler için kısıtlama kayıtlarını içerir. Bu kısıtlar, kullanıcının işlemleri gerçekleştirmesi esnasında, yetkisinin kontrolünde yetki denetim mekanizmasını destekler. Yetki denetim mekanizması, bu listeleri kontrol ederek işlem üzerinde bir kısıt varsa kullanıcıya bu kuralı uygular. Bu, sistem ve işlem temelli, çoklu kontrol, daha güvenilir bir yetki denetimi mekanizması olma amacı taşır. Oysa liste tabanlı yetki denetimi, hala yetki denetimini istenen seviyeye taşıyamamaktadır.

Listeler, kullanıcılar için sistem işlemleri üzerinde "izin" veya "ret" gibi temel ve sınırlı kısıtlamaları içerebilmekte ve iş akışında yer alan işlemler karmaşıklaştığında bu kısıtlar yetersiz kalmaktadır [9]. Örneğin, kurumsal yapıda, bir alım görevlisinin satın alma ile ilgili izinleri, "yapabilir" veya "yapamaz" şeklinde kesin çizgilerle belirlenmesi iş süreci içinde boşluklar oluşturur. Satın alma izni yetkisindeki miktarı belirleyen sınır değeri, liste yönteminde belirsizdir. İş sürecinde, yetkili, belirli miktarlara göre alım onayı verebilir. Ama alım miktarı, sınır değerini aştığında alım, bir üst yetkilinin onayına bağlıdır. Kurumsal yapı ve iş akışı listelerin bu tip detaylı tanımlamalarla güncellenmesini gerektirir. Bu yaklaşım ise listelerin yönetim ve kontrolünü zorlaştırmaktadır [9].

Rol tabanlı erişim denetimi yöntemleri(RBAC) [10], [23] erişim kontrol listelerinin eksikliklerini önlemek için önerilmiştir. Kullanıcıları, kurumsal rolleriyle gruplandırarak, işlemlerin bu gruplara tanımlı izinler doğrultusunda gerçeklenmesini destekler. Bir rol, aynı pozisyona sahip veya aynı işlemleri gerçekleştiren kullanıcı grupları olarak tanımlanmaktadır [23]. Rollerin iş akışına uygun olarak genişlemesi, üst seviyeye çıkarılması veya düşük seviyeye indirgenmesi gibi hareketleri kolaylıkla ve verimli şekilde gerçekleştirilmektedir. RBAC aynı zamanda rollerin devredilmesi olanağı sağlar [30].

Öznitelik tabanlı erişim kontrolü ABAC[31] ise RBAC'ın dinamik bir ortamda problemlerine çözüm olarak sunulan bir diğer erişim kontrol mekanizmasıdır. ABAC,

işlemlerin gerçekleştirilme yetkileri için nesnelere zaman, yer gibi dinamik özniteliklerin tanımlanmasını içerir. Bununla birlikte ABAC yönteminde bir rol sadece rol ismi olarak tanımlanır ve bu tanım, izinleri içermez. Bu yaklaşım, kullanıcılar için tanımlanan roller için dinamizmi sağlamakla birlikte yetki denetimi mekanizması rol öznitelikleri üzerinden izinlerin sorgulanması gerekmektedir. Oysa RBAC rol tanımlarının yetki denetim mekanizmasında role göre tanımlı izinleri çıkarması kolaydır. ABAC yaklaşımının sadece RBAC'ın dinamik yönetim problemlerini çözümlemek olarak yapılandırılması, önerilen modelde erişim denetim modeli olarak her iki yaklaşım yerine yetki denetiminde daha etkin olan RBAC'ın yer alması tercih edilmiştir. ABAC'ın yer almaması tercihi, bir olumsuzluk yaratmamakla beraber modelin odaklandığı amaca uygunluğunu sağlamak açısından yapılmıştır.

Önerilen çok-katmanlı model, iş akışındaki yetki denetim mekanizmalarını analiz eder. Katmanlı yapı, her bir mekanizmayı yetki denetiminde yetenekleri, yetkinlikleri ve iş akışındaki dokümanların güvenilirliğine katkıları kapsamlarında ayrı katmanlarda ele almıştır.

Literatürde katmanlı yetki denetim mekanizması yaklaşımlarından biri de OAuth'tur [32]. Bu yaklaşımda önerilen yetki denetim çerçevesi, üçüncü tarafların bir HTTP hizmetine erişimini sınırlayan bir yetki katmanı sağlar. OAuth çerçevesi, bir uygulamanın kullanıcısının yetkilerine ihtiyaç duyduğu ve kullanıcının uygulamaya kimlik bilgilerini girmesi gerektiği durumlardaki yetki problemlerini hedefler. Bu gibi durumlar, yetkinin iptali veya kullanıcı kimlik bilgilerinin açığa çıkması gibi sorunlar çıkarabilmektedir. Yetki katmanı istemcinin rolü ile kaynak sahibini ayırma işlevini üstlenir. RFC dokümanında belirtildiği gibi, OAuth çerçevesinin http dışındaki protokollerde kullanılması yapının amacı dışındadır. Çok katmanlı yetki modeli, iş akışlarındaki yetki denetim mekanizmalarını temel aldığından, OAuth'un kapsamı iş akışlarına doğru genişlemediği müddetçe OAuth'u kapsam dışı bırakmaktadır.

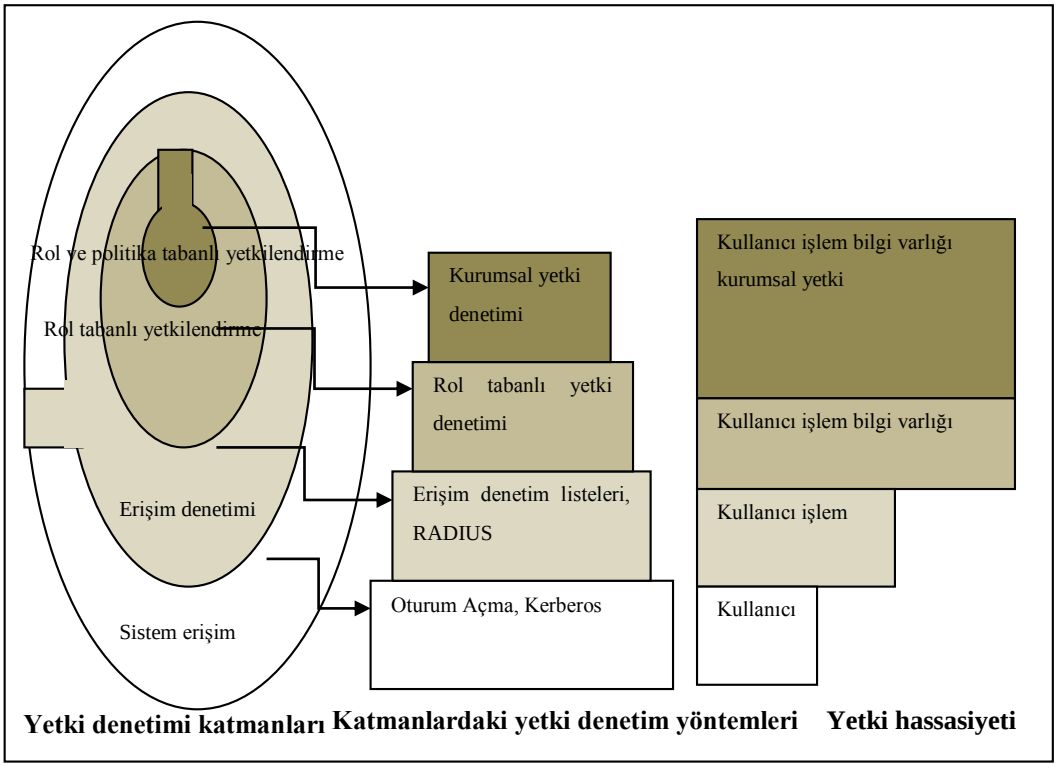
Kurumsal bilgi güvenliğinin ve uygulanan güvenlik politika ve protokollerin yeterliliklerinin araştırılması ve testi için birçok yöntem ve uygulama vardır. Literatürde, iş akışlarının modellenmesi ve protokol güvenlik analizinde kullanılan Petri ağları [33], [34], [35] bu çalışmada sürdürülebilirlik ve erişilebilirlik analizinde kullanılmıştır. Örnek vakada üretilen çözüm önerisinde ise eşleme tabanlı kriptografi [36], [37]' den faydalanılmaktadır.

3. ÖNERİLEN MODEL

Yetki denetimi, kullanıcıların sistem üzerindeki izinlerini belirleyerek, kullanıcıları bu izinlere uygun olarak işlem yapmaya zorlayan bir güvenlik mekanizmasıdır. Bu tezde, yetki denetim mekanizmalarını temel alan ve genel yapısı Şekil 3.1'de verilen, çok katmanlı bir yetki denetim modeli sunulmaktadır. Katmanlar, yetki denetiminin işlevleri ve hassasiyetlerine göre yapılandırılmıştır.

Yetki denetim mekanizmaları, modelde alt katlardan üst katlara çıkıldıkça kullanıcıyı daha kesin ve hassas bilgiler ile sınayarak daha özel süreçlere dâhil etmektedir. Her bir katmanda sorgulanan yetki bilgisi, bir filtre işlevi görmekte ve kullanıcıyı bir üst katmana taşımaktadır. Yetki katmanları, kurumsal iş akışında gereksinim duyulan yetki denetimi için temel yapıları içermektedir.

Yetki katmanlarındaki yetki denetimi yöntemleri, yetki denetim uygulamalarında çözüm olarak sunulan mekanizmalardan oluşmaktadır. Yetki hassasiyeti, her katmanda gereksinim duyulan yetki bilgisi ile şekillenen filtrelerdir. Kurumsal iş akışındaki varlık, ilgili katmanda bir işlem gerçekleştirmek veya bir sürece erişmek için bu bilgiyi sağlamalıdır.



Şekil 3.1: Çok Katmanlı Yetki Denetim Modeli

3.1. Modele Genel Bir Bakış

Bu bölümde, çok katmanlı yetki denetim modeli, her bir katmanın yetki kapsamı ve o katmanda yer alan mekanizma sunularak kısaca özetlenmektedir.

- Sistem Erişim Katmanı

Çok katmanlı yetki denetim modelinin ilk katmanı olan sistem erişim katmanı, genel sistem giriş yetkisini içerir. Sistem erişimi için yapılan yetki denetimi, kimlik doğrulama mekanizmasından oluşmaktadır. Bu katmanda, izin için kimlik bilgisi ve parolaya ihtiyaç duyulmaktadır. Bu katman, tüm kullanıcılara uygulanır. Yetki denetim hassasiyeti düşük olduğundan kontrol için sadece kullanıcı bilgisi kullanılır. Bununla birlikte, kullanıcıya yetki denetimi sonucunda verilen izin kapsamı geniştir. Kullanıcıya, ya tüm sisteme erişim izni ya da erişim için mutlak ret kuralları uygulanır. Sisteme erişimi sağlanan kullanıcılar için başka bir işlemsel kısıtlama uygulanmamaktadır. Temel oturum açma, Kerberos ve RADIUS kimlik doğrulama uygulamaları bu katmanda yer alan uygulamalardır. İki katmanlı Kerberos kimlik doğrulama ve oturum bileti üretimi üst katmanlara kıyasla düşük bir yetki denetim karmaşıklığı içerir. Güvenlik seviyesinin artırılmasında, sınama sürecinde genel olarak kriptografik algoritmalar kullanılmaktadır.

- Erişim Denetim Katmanı

İkinci katmanda, ilk katman sonucunda sisteme erişim hakkı kazanmış kullanıcılar için işlemler bazında yetki denetimi sağlanır. RADIUS yetki denetim mekanizması ve erişim kontrol listelerindeki gibi kullanıcıların izinleri, işlemler bazında erişim denetim listelerinden sorgulanır. İşlemler, yetkilere göre onay veya ret ile sonuçlanır. Bu katman, ilk katmana kıyasla daha dar bir kullanıcı grubuna uygulanır. Bu kullanıcı grubu, ilk katmandan filtrelenerek sisteme erişim hakkı kazanan kullanıcılardan oluşur. Yetki denetimi, ilk katmana kıyasla daha belirlidir. Listeler, kullanıcı, işlem ve "onay/ret" ifadelerini içerir. Katman, bu bilgiler ile işlem temelli yetki denetimi sağlar. Her ne kadar erişim denetim listeleri ile sınırlı olsa da sağlanan güvenlik seviyesi yüksektir. Sistem genelinde erişime kıyasla, bu katmandaki mekanizma, yetki denetim kapsamını işlem özeline indirmektedir.

- Rol Tabanlı Yetkilendirme Katmanı

Üçüncü katman, rol tabanlı yetki kontrol katmanıdır. Bu katmanda, kullanıcılar, iş akışı sürecinde rollerine göre gruplandırılmaktadır. Bu yaklaşım, erişim denetim listelerinin eksikliklerine çözüm olarak önerilmektedir. Bu yetkiler sadece işleme bağlı değildir. İşlemin gerçekleştirilme kurallarını da içermektedir. Daha önce belirtildiği gibi, bir rol, aynı işlemi gerçekleştiren veya aynı görevi paylaşan kullanıcılar grubudur. Rol, kullanıcıya işlemi gerçekleştirmesi için atanır. İkinci katmandaki bir kullanıcının kullanıcıdan yöneticiye yükseltilerek gereksiz genişlikte yetkiyle donatılmasındansa, belirlenmiş bir rolün kullanıcıya atanması daha güvenlidir. Bu yaklaşım, kurumsal yapıda rollerin yönetimine de izin verir. Kullanıcı ve rolü, kolaylıkla terfi, iptal edilebilir veya vekâlet verilebilir. Bu katmanda, kullanıcı-grup-işlem ve bilgi varlığı kullanıldığından yetki hassasiyeti yüksektir. Yetki denetiminin kapsamı işlem ve bilgi varlığı ile belirlenir. Yetki denetimi, gerçekleştirilmek istenen işlemin hangi şart ve hangi izin ile onaylanacağı ile ilgilidir.

- Rol ve Politika Tabanlı Yetkilendirme Katmanı

Modelin bu en üst katmanı rol tabanlı yetkilendirme üzerinde dördüncü bir katman olarak tanımlanmıştır. Bu katman kurumsal yetki denetimi mekanizmalarını hedefler. Rol tabanlı mekanizmanın kurumsal yapıda yetersiz kaldığı durumlarda, yetki denetimi kurumsal politika, yönetmelik ve kılavuzları içerecek kadar etkin olmalıdır.

Örnek bir durum olarak, kurumsal yapıda, bir çalışanın bir malın satın alımı ve alım belgesini onaylama rolleri olsun. Bu süreç sonunda satın alma işlemi tamamlanmış olacaktır. Gerçekte, kurumsal bir politikada satın alma işi "eğer ödeme miktarı belirli sınırın üzerindeyse alım belgesi daha üst yetkili tarafından onaylanmalıdır" şeklinde tanımlanır. Yetki denetimi kurumsal politikayı göz önünde bulundurmalı ve yetki bilgisi politikada belirlendiği gibi süreçte karşılık bulmalıdır.

Bir işlemin, kimin tarafından, nasıl gerçekleştirileceği ve kurumsal iş akışının hangi aşamasında yer aldığı gibi öznitelikleri yetkilerin belirlenmesi açısından önem taşır. İlk katmanda, genel yetki için kimlik bilgisi kullanılmaktadır. Üst katmanlarda ise erişim listeleri, rol tabanlı ilişkiler gibi ek bilgiler gerektirmektedir. Kurumsal yapıda, rol tabanlı yetki denetimi Görevlerin Ayrımı (SoD) [23] ilkesinin kullanılmasını önerir. Bu kural, yukarıda verilen durumda satış ve alım rollerine

uygulanır. Rol tabanlı yaklaşım, ilgili prosedürleri yetkilendirme ve ayırma konusunda verimlidir. Fakat kurumsal kılavuz ve yönergeler, rollerde tanımlı değildir. Bu sebepten, üretilen belge için bu yetkilerin doğrulanması da söz konusu olamamaktadır.

Bu katmanda, yetki hassasiyeti en üst noktadadır, mekanizma kimlik doğrulama, işlem ve rol yanında kurumsal yönergeleri de denetler. Yetki denetiminin karmaşıklığı da aynı oranda yüksektir. Yetki denetimi, işlemlerin özniteliklerini kapsamaktadır.

3.2. Petri Ağı ile İş Akışları Üzerinde Yetki Denetim Katmanlarının Modellenmesi

Bu bölümde, modelde yer alan her bir yetki denetim katmanı, kurumsal iş akışında Petri ağları kullanılarak gösterilmiştir. Her bir katmandaki yetki denetiminin kapsamı ve mekanizmalar bu iş akış modelleri yardımıyla incelenmiştir.

Petri ağları ile kurulan modeller, bir varlığın yetki denetimi karşısında, yetkisinin gözlemlenmesi açısından kullanışlı olmaktadır. Eğer bir varlık, ağdaki herhangi bir noktaya erişebiliyorsa, iş akışında o noktadaki durumu gerçekleyebilir, o noktadaki işlemi gerçekleştirebilir. Petri ağlarındaki erişilebilirlik aşağıdaki gibi tanımlanıp kullanılabilir:

U Sistemde tanımlı kullanıcılar kümesi $u_i, u_{id} \in U$; u_i sistemdeki herhangi bir kullanıcı, u_{id} ise sistemde tanımlı, kimliği doğrulanmış bir kullanıcı olsun. Eğer, P_n yeri u_{ix} için Petri ağında erişilebilir ise, kullanıcı u_{ix} P_n yerindeki işlemi gerçekleştirmeye yetkilidir.

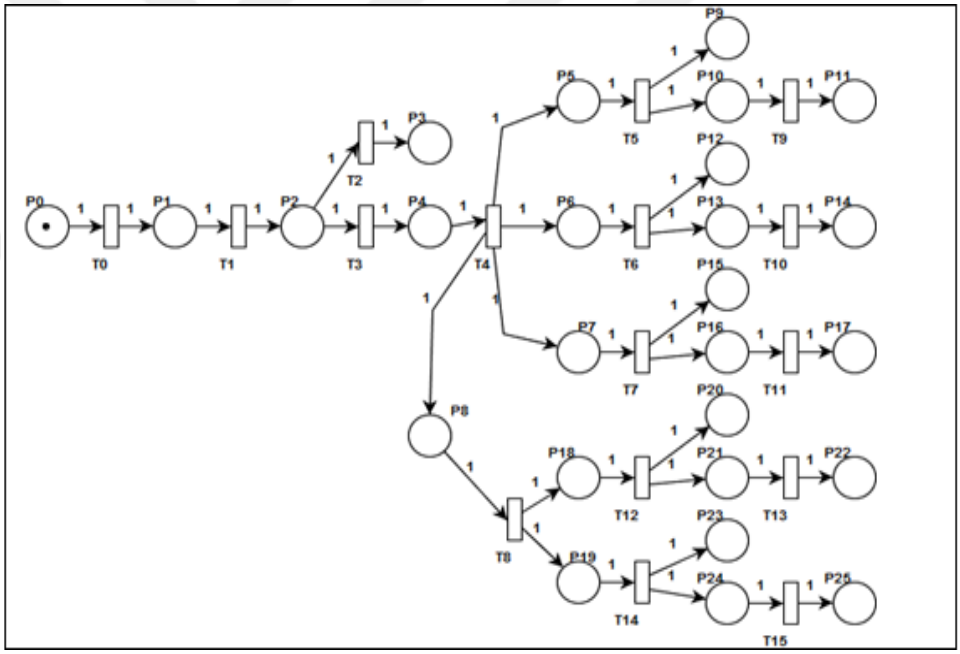
Daha önce çok katmanlı modeldeki katmanların, yetki denetimindeki hassasiyetleri ve işlevlerine göre yapılandırıldığı belirtilmişti. Her bir katman için oluşturulan temel Petri ağı modellerinde, işlevler, iş akışındaki geçiş ve yerler ile tanımlanmaktadır. Yetki denetimindeki hassasiyet ise yetki denetimi için gereksinim duyulan bilgi paketi ile temsil edilmiştir. Bir işlem, gerçekleştirilebilmesi için gereksinim duyulan bilgi {*işlem, işlem tipi, kullanıcı tipi, kullanıcı, yetki bilgisi*} özelliğinde 5'li bir bilgi kümesi ile tanımlanmıştır. Eğer farklı durumlarda yetki denetimi için bir bilgiye ihtiyaç duyulmuyorsa veya ilgili durumda o bilgi yoksa o bilgi $\emptyset$ ile gösterilmektedir. Gereksinim duyulan yetki bilgisi ise parantezler ile vurgulanmaktadır.

$U = \{u_1, u_2, \dots u_a, \dots, u_m, \dots u_z\}$ Sistemde tanımlı kullanıcılar kümesi

$u_a, u_m \in U$; u_a herhangi bir yetkili kullanıcıyı, u_m, yetkisiz kullanıcıyı temsil etsin. u_m erişebildiği dokümanlarla sistem akışını, güvenilirliğini bozacak iç saldırgan, v, sistemde kullanıcı olarak tanımlanmayan dış saldırgan olsun. Saldırganın başlangıçta hiçbir bilgiye sahip olmadığı varsayılmıştır.

$D = \{d_1, d_2, \dots, d_a, d_c, d_s, d_o, d_u, \dots, d_y\}$ dolaşımdaki doküman kümesi olmak üzere; d_n herhangi bir dokümanı, d_c oluşturulmuş, d_u güncellenmiş/düzenlenmiş, d_s ise imzalanmış ve onaylanmış, d_a arşivlenmiş ve d_o kurum dışına yazılan bir dokümanı temsil etmektedir.

Kurumsal iş akışı kapsamında, sisteme giriş, bir belgenin oluşturulma, onaylanma süreci ve bu sürecin sonundaki olası arşivlenme ve kurumlar arası yazışma işlemlerini içerecek şekilde modellenen ve Şekil 3.2'de sunulan Petri ağına ait yer ve geçişler Tablo 3.1'de verilmiştir.



Şekil 3.2: Kurumsal iş akışında yetki denetiminin Petri ağ modeli

- Çok Katmanlı Yetki Denetim Modelinin İlk Katmanı

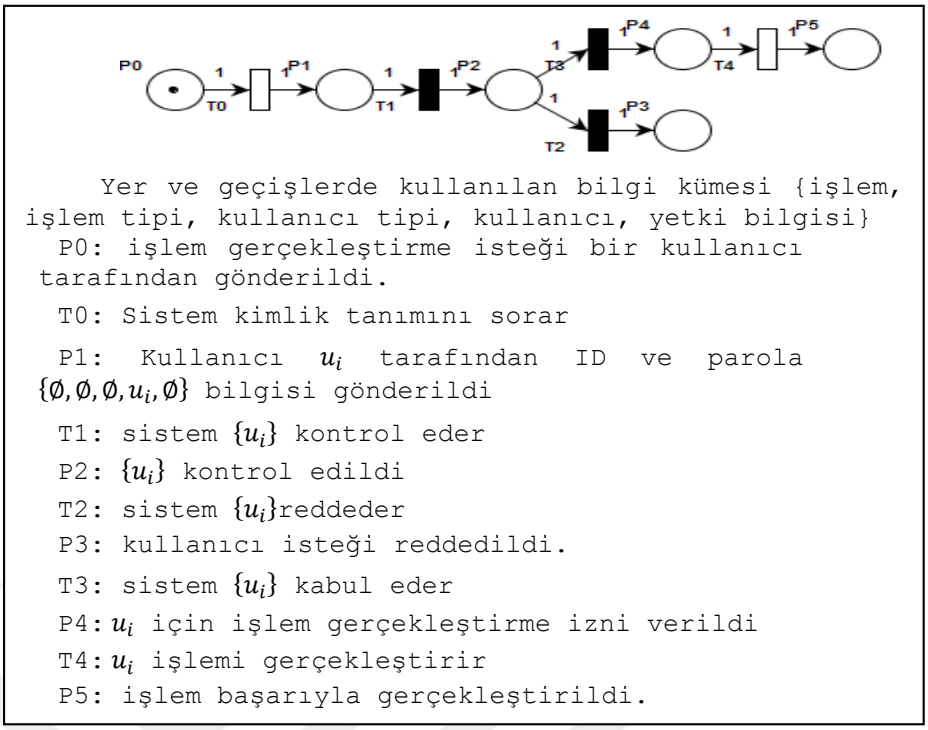
Yetki denetimi kullanıcıya sistem genelinde uygulanır. Kimlik doğrulama mekanizması bu katmanda gerçekleşir. Kullanıcı bu katmanda elde ettiği yetkiyle sistem genelinde tüm işlemleri gerçekleştirebilir. Örnek yöntem ve uygulamalar: Kullanıcı oturum açma ve Kerberos kimlik doğrulama.

• Kullanıcı Oturum Açma

Oturum açma mekanizması Şekil 3.3'de sunulan Petri ağı ile modellenmiştir. $M_2 \xrightarrow{t_3} M_4$ sırası ile $\{p_2, p_4\}$ yerlerinden geçebilen, başka bir deyişle p_5 i tetikleyebilen kullanıcı, sistemde herhangi bir işlemi gerçekleştirebilir. İlk işaret $[1000000]$ durumunda, kullanıcı $u_i, [t_0\, t_1\, t_3\, t_4\,]$'ü tetikler. Tablo 3.2 deki çakışıklık matrisi uyarınca, $M = M_0 + \mu I$ formülünden kullanıcı u_i nin erişilebilirliği $[000001] = [1000000] + [11011] \cdot I$'dir. Kullanıcının p_5'e erişebildiği mümkün olan sonuç sırası $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_3} M_3 \xrightarrow{t_4} M_4$ 'dır.

Tablo 3.1: Petri ağı modeline ait yer ve geçişler

P0: Kullanıcı tarafından sistem erişimi isteği iletildi.	*P13*: Kullanıcıya belge düzenleme izni verildi.
T0: Sistem kullanıcı için kimlik doğrulama yapar.	*T10*: Kullanıcı belgeyi düzenler.
P1: Kullanıcı kimlik bilgilerini{ID, parola}sisteme iletti.	*P14*: Belge değiştirildi.
T1: Sistem kimlik bilgilerini denetler.	*T7*: Belge onaylama için kullanıcı yetkisi denetlenir.
P2: Kullanıcı kimliği denetlendi.	*P15:* Kullanıcıya belge onaylama izni verilmedi.
T2: Sistem kullanıcıyı kabul etmez.	*P16*: Kullanıcıya belge onaylama izni verildi.
P3: Kullanıcıya erişim izni verilmedi.	*T11*: Kullanıcı belgeyi onaylar.
T3: Sistem kullanıcıyı kabul eder.	*P17:* Belge onaylandı.
P4: Kullanıcı sisteme dâhil oldu.	*T8*: Belge aktarımının hedefi belirlenir.
T4: Kullanıcı işlem seçimi yapar.	*P18*: Kullanıcı belge arşivlemeyi seçti.
P5: Kullanıcı belge oluşturmayı seçti.	*P19*: Kullanıcı kurumlar arası belge iletimini secti.
P6: Kullanıcı belge düzenlemeyi seçti.	*T12*: Belge arşivleme için kullanıcı yetkisi denetlenir.
P7: Kullanıcı belge onaylamayı seçti.	*P20*: Kullanıcıya belge arşivleme izni verilmedi.
P8: Kullanıcı belge aktarımını seçti.	*P21*: Kullanıcıya belge arşivleme izni verildi.
T5: Belge oluşturma için kullanıcı yetkisi denetlenir.	*T13*: Belge arşivlenir.
P9: Kullanıcıya belge oluşturma izni verilmedi.	*P22*: Belge arşivlendi.
P10: Kullanıcıya belge oluşturma izni verildi.	*T14*: Kurumlar arası belge iletimi için belge uygunluğu ve kullanıcı yetkisi denetlenir.
T9: Kullanıcı belge oluşturur.	*P23*: Kurumlar arası belge iletimi için izin verilmedi.
P11: Belge oluşturuldu.	*P24*: Kurumlar arası belge iletimi için izin verildi.
T6: Belge düzenleme için kullanıcı yetkisi denetlenir.	*T15*: Kurumlar arası belge iletimi gerçekleşir.
P12: Kullanıcıya belge düzenleme izni verilmedi.	*P25*: Belge iletildi.



Yer ve geçişlerde kullanılan bilgi kümesi {işlem, işlem tipi, kullanıcı tipi, kullanıcı, yetki bilgisi}

P0: işlem gerçekleştirme isteği bir kullanıcı tarafından gönderildi.

T0: Sistem kimlik tanımını sorar

P1: Kullanıcı u_i tarafından ID ve parola $\{\emptyset, \emptyset, \emptyset, u_i, \emptyset\}$ bilgisi gönderildi

T1: sistem $\{u_i\}$ kontrol eder

P2: $\{u_i\}$ kontrol edildi

T2: sistem $\{u_i\}$reddeder

P3: kullanıcı isteği reddedildi.

T3: sistem $\{u_i\}$ kabul eder

P4: u_i için işlem gerçekleştirme izni verildi

T4: u_i işlemi gerçekleştirir

P5: işlem başarıyla gerçekleştirildi.

Şekil 3.3: Oturum açma Petri ağı modeli

Tablo 3.2: İlk katman Petri ağı için çakışıklık matrisi

İleri çakışıklık matrisi I^+

	T0	T1	T2	T3	T4
P0	1	0	0	0	0
P1	0	1	0	0	0
P2	0	0	1	1	0
P3	0	0	0	0	0
P4	0	0	0	0	1
P5	0	0	0	0	0

Geri çakışıklık matrisi I^-

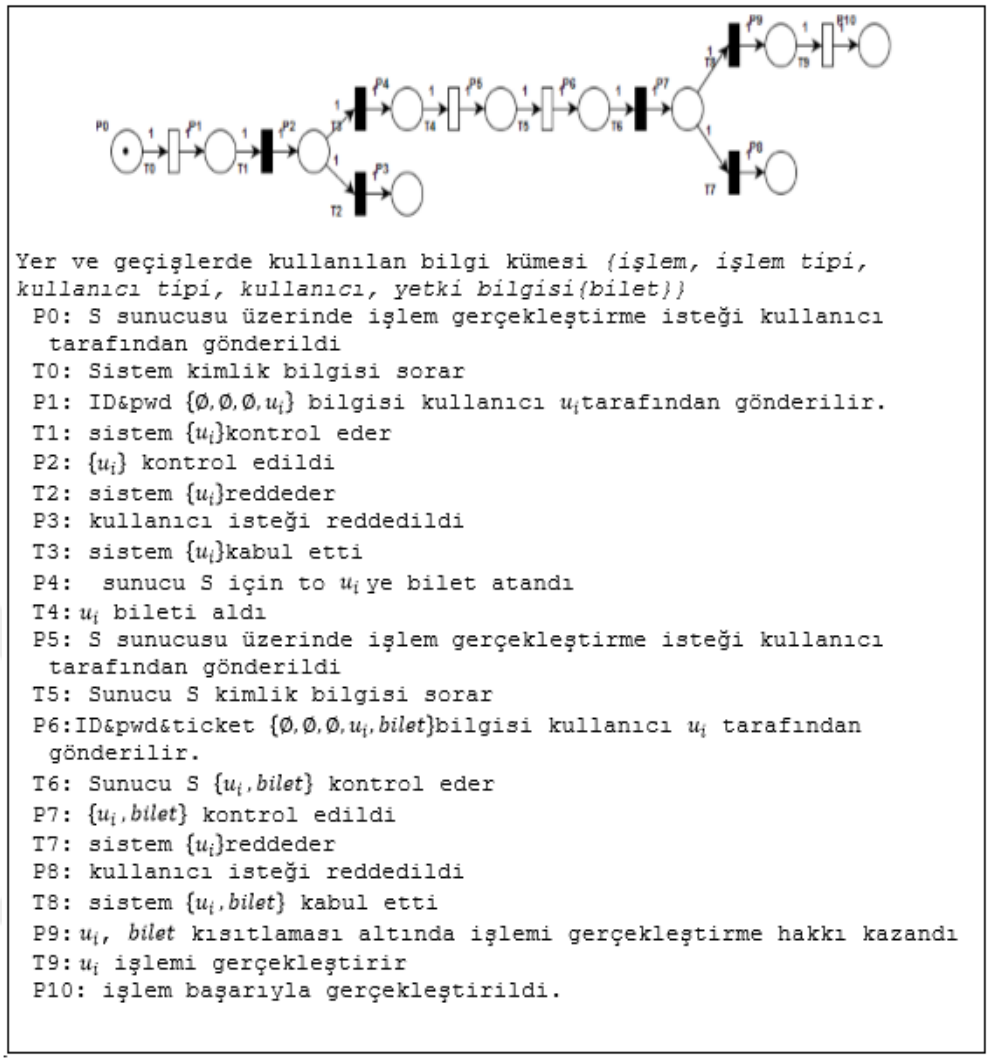
	T0	T1	T2	T3	T4
P0	1	0	0	0	0
P1	0	1	0	0	0
P2	0	0	1	1	0
P3	0	0	0	0	0
P4	0	0	0	0	1
P5	0	0	0	0	0

Birleşik çakışıklık matrisi I

	T0	T1	T2	T3	T4
P0	-1	0	0	0	0
P1	1	-1	0	0	0
P2	0	1	-1	-1	0
P3	0	0	1	0	0
P4	0	0	0	1	-1
P5	0	0	0	0	1

- Kerberos Yetki Denetim Mekanizması

Mekanizma, temel oturum açma yapısını genişletmektedir. Kimlik doğrulama işlemi, kimlik doğrulama sunucusunda gerçekleşir. Eğer istek onaylanırsa kullanıcıya belirli bir süre için sunucuya erişim izni verilir. Bu mekanizmaya ait temel Petri ağı modeli Şekil 3.4'te sunulmaktadır. Kullanıcı u_i, p_{10} a $[t_0 t_1 t_3 t_4 t_5 t_6 t_8 t_9]$ geçişleri sonucunda erişir. Kullanıcı u_i nin erişilebilirliği $[00000000001] = [1000000000] + [1101111011] \cdot I$'dir. Kullanıcının p_{10}'e erişebildiği mümkün olan sonuç sırası $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_3} M_3 \xrightarrow{t_4} M_4 \xrightarrow{t_5} M_6 \xrightarrow{t_6} M_7 \xrightarrow{t_8} M_8 \xrightarrow{t_9} M_9$ dır.



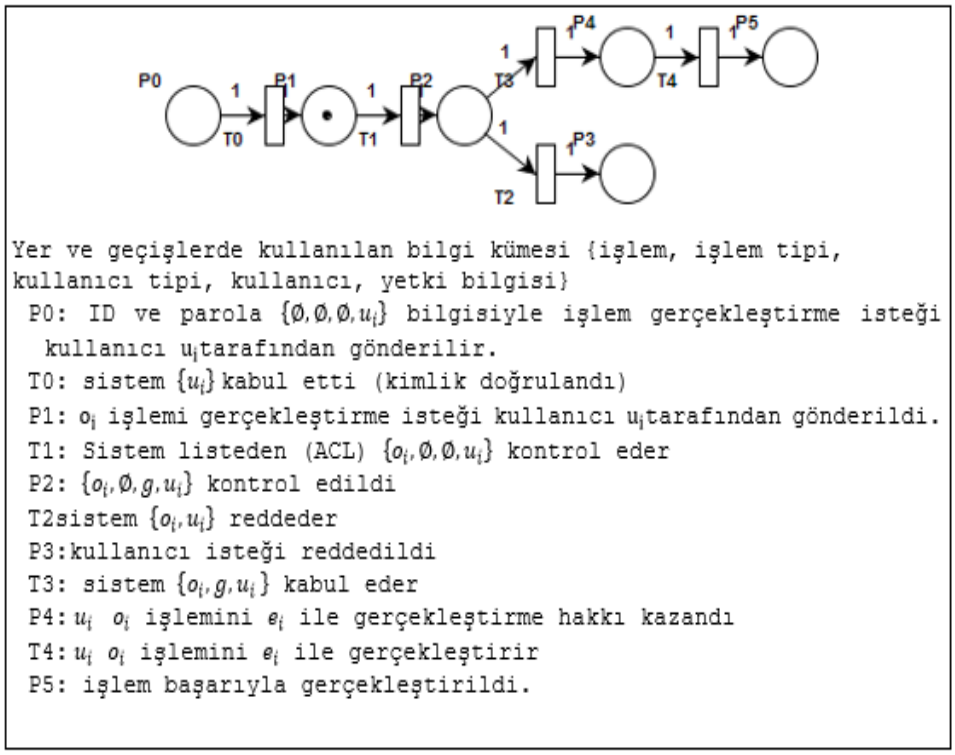
Şekil 3.4: Kerberos Petri ağı modeli

• Çok Katmanlı Yetki Denetim Modelinin İkinci Katmanı

Kimlik doğrulamasından geçmiş kullanıcıların geniş yetkilerini kullanarak iş akışını olumsuz yönde değiştirebilecekleri işlemleri kısıtlamak için gerçekleştirilen temel erişim denetimi ve yetki denetimi mekanizması bu katmanda yer almaktadır. Kontrol listeleri, kullanıcıların sistem genelinde yapacağı işlemlere erişim kısıtlaması getirmek için tasarlanmıştır.

İkinci katmanda, ilk katmandan farklı olarak kullanıcı grubu ve işlem kuralı ile tanımlanan kayıtların bulunduğu erişim kontrol listeleri yer alır. Bu listeler katmanın yetki denetim hassasiyetini belirler. Bu listeler, *<kullanıcı/grup, işlem, "onay/ret" >* ile tanımlanan izinleri içerir. Amaç, iş akışındaki kullanıcıların yetkisiz işlem

gerçekleştirmesini engellemektir. Erişim kontrol listelerini örnekleyen Petri ağı modeli Şekil 3.5'de sunulmaktadır.Yetki denetiminin ilk katmanı M_0 işareti ile temsil edilmektedir. İkinci katman M_1 ile başlamaktadır.



Şekil 3.5: Erişim denetim listesi tabanlı yetki denetimi Petri ağı modeli

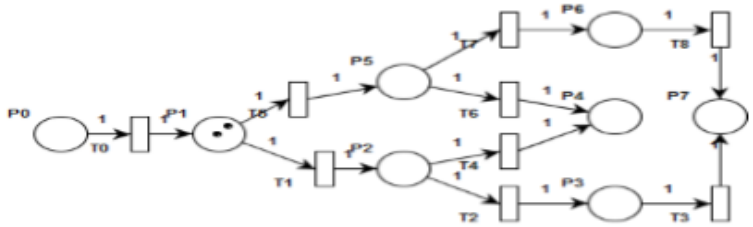
Kimliği doğrulanmış kullanıcı u_{id} $[t_0\, t_1\, t_3\, t_4]$:[11011] ü tetikleyebilir. [100000] ilk işareti ile erişilebilirlik $[000001] = [100000] + [11011] \cdot I$ olmaktadır. Kullanıcı u_{id} P5'e $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_3} M_3 \xrightarrow{t_4} M_4$ sırası sonucunda erişir. p_5'de kullanıcı u_{id} erişim kontrol listesinde tanımlanan $\{o_i, g, u_{id}\} \rightarrow onay$ kuralına uygun olarak o_i işlemini gerçekleştirir. Kullanıcı u_{id}, P5'de $\{u_{id}, o_{onay}\}$ işlemini $P2$'de elde ettiği $\langle şefler, o_{onay}, izinver\rangle \wedge u_{id} \in şefler$ kuralı ile gerçekleştirebilmektedir.

• Çok Katmanlı Yetki Denetim Modelinin Üçüncü Katmanı

Bu katman önceki katmandaki yetki denetim zafiyetlerini çözümleyerek sistemin yetki denetim yeteneklerini artırmanın amaçlandığı rol tabanlı kontrol mekanizmaları üzerine kurulmuştur. Yetki denetimi roller ve bu rollere tanımlı izinleri temel alır. Ikinci katman, dosya, veritabanı veya donanım gibi alt seviye erişimlere

uygulanırken; bu katman iş akışındaki işlemler için özelleşmiştir. Mekanizma işlemler üzerinde daha detaylı tanımlarla kontrolü sağlar.

Çok katmanlı yapı, işlemlerin yetki gereksinimlerine göre filtreleme yapılmasına olanak sağlayarak yönetim yükünü azaltmaktadır. İlk katman yetkisiz kullanıcıların sisteme erişimlerini önlemektedir. İkinci katman alt seviye işlemler için kısıtlamalar getirirken; üçüncü katman iş akışındaki işlemler için yetki denetimini sağlar. Üçüncü katman yetki denetimi mekanizmalarını örnekleyen temel rol tabanlı yetki denetim mekanizmasına ait Petri ağı modeli Şekil 3.6'da sunulmaktadır.



Yer ve geçişlerde kullanılan bilgi kümesi {işlem, işlem tipi, kullanıcı tipi, kullanıcı, yetki bilgisi}

P0: ID ve parola $\{\emptyset, \emptyset, \emptyset, u_i\}$ bilgisiyle işlem gerçekleştirme isteği kullanıcı $u_i$tarafından gönderilir.
T0: sistem $\{u_i\}$ kabul etti (kimlik doğrulandı)
P1: o_i işlemi gerçekleştirme isteği kullanıcı $u_i$tarafından gönderildi.
T1: Sistem listeden (ACL) $\{o_i, e_i, \emptyset, u_i\}$ kontrol eder
P2: $\{o_i, \emptyset, g, u_i\}$ kontrol edildi
T2: Sistem $\{o_i, g, u_i\}$ kabul eder
P3: u_i o_i işlemini e_i ile gerçekleştirme hakkı kazandı
T3: u_i o_i işlemini e_i ile gerçekleştirir
T4:Sistem $\{o_i, u_i\}$ reddeder
P4:kullanıcı isteği reddedildi
T5:Sistem kullanıcı rolleri ve işlem kurallarından $\{o_i, e_i, r, u_i\}$ kontrol eder
P5: $\{o_i, e_i, r, u_i\}$ kontrol edildi
T6:Sistem $\{o_i, e_i, r, u_i\}$ reddeder
P4:kullanıcı isteği reddedildi
T7: Sistem $\{o_i, e_i, r, u_i\}$ kabul eder
P6: u_i r rolü ile o_i e_i işlemini gerçekleştirme hakkı kazandı
T8: u_i r rolü ile o_i e_i işlemini gerçekleştirir
P7: işlem başarıyla gerçekleştirildi.

Şekil 3.6: Rol tabanlı yetkilendirme Petri ağı modeli

Yetki denetiminin ilk katmanı M_0 işareti ile temsil edilmektedir. İkinci katman M_1 ile başlamaktadır. Eğer işlem, listede yer almıyorsa yetki denetim kararı ret veya tanımsız yerine rol tabanlı yetki denetim mekanizması tarafından verilecektir. Yetki

denetiminin üçüncü katmanı $M_2 \xrightarrow{t_5}$ ile başlamaktadır. Sistem, ağ üzerinde yer p_4 ve yer p_7'de sonlanmaktadır.

Kimliği doğrulanmış kullanıcı u_{id},$[t_0\, t_5\, t_7\, t_8\,]$:$[100001011]$ tetikleyebilir. $[10000000]$ işareti ile erişilebilirlik $[0000001] = [10000000] + [100001011] \cdot I$ olmaktadır. Kullanıcı u_{id}, yer P7'ye $M_0 \xrightarrow{t_0} M_2 \xrightarrow{t_5} M_3 \xrightarrow{t_7} M_4 \xrightarrow{t_8} M_5$ $\{p_0, p_1, p_5, p_6, p_7\}$ üzerinden erişir. Yer P7'de kullanıcı u_{id}, eğer u_{id}'nin r rolünün gerçekleme izni varsa o_i işlemini gerçekleyebilir. Kullanıcı u_{id} yer P7'deki $\{u_{id}, o_{onay}\}$ işlemini "$satın\ alma\ birim\ şefi$" rolünde tanımlı izinle $\langle şefler, o_{onay}, izinver\rangle \wedge$ u_{id} satın alma birim şefi $rolüne\ sahiptir$ yetkisine uygun olarak gerçekleştirir.

Yetki denetim modelinin ilk aşaması $M_0 \xrightarrow{t_0}$ başlangıç işaretiyle başlayan ve $M_2 \xrightarrow{t_2}$ veya $M_2 \xrightarrow{t_3}$ ile sonuçlanan kimlik denetimini içerir. Bu aşamada sisteme giriş ve sistem kaynaklarını kullanma izni $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_3} M_3$ geçiş dizisinin gerçeklenmesi ile mümkün olacaktır.

Erişilebilirlik analizine göre sistemde tanımlı olmayan dış saldırgan v, kimlik denetiminden geçemediği için: $[T0, T1, T2]$ tetiklenecektir, durum $[11100..0]$ ve başlangıç işareti $[10000..0]$ olmak üzere, komşuluk matrisi $I, M = M0 + \mu I$ yardımıyla, geçiş dizisi $[000100..000] = [1000..0] + [11100..0].I$ olarak sonuçlanır. v, ancak $P3$'e erişir ve sisteme girişi reddedilir. İş akışı v için $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_3} M_3$ dizisi ile sonlanır.

Sistemde tanımlı kullanıcılar $u_n, u_a, u_m \in U$ için kimlik denetimi ile sağlanan erişilebilirlik ise $[T0, T1, T3]$ tetiklenmesi sonucu, durum $[1101\ldots]$ ve başlangıç işareti $[1000..0]$ olmak üzere, geçiş dizisi $[00001..] = [1000..0] + [1101..].I$ olmaktadır. İş akışında bu aşamanın devamında başka bir yetki kontrolü olmadığı bir durumda $u_i, u_a, u_m \in U$ kullanıcıları $d_n, d_a, d_c, d_s, d_o, d_u \in D$ dokümanlarına erişebilir veya oluşturabilirler.

Yetkilendirmenin ikinci aşaması $M_3 \xrightarrow{t_3} M_4 \xrightarrow{t_x}$ile başlamaktadır. Bu aşamada kullanıcılara tanınan yetkiler daraltılarak, işlemleri gerekli izinler doğrultusunda gerçekleyebilme yetkisi verilir. İş akışında işlemlere göre $T5, T6, T7, T12$ ve $T14$ tetiklemeleriyle bu yetki denetimleri gerçekleştirilmektedir.

Belge oluşturma yetkisi olan bir kullanıcı, u_a, $[T0, T1, T3, T4, T5, T9]$ tetiklenmesi sonucu, durum $[1101110001]$ ve başlangıç işareti $[1000..0]$ ile M_0 $\xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_3} M_3 \xrightarrow{t_4} M_4 \xrightarrow{t_5} M_5 \xrightarrow{t_9} M_6$ dizisi sonucu $P11$'e erişebilecek ve işlemi gerçekleştirebilecektir. Belge oluşturma yetkisine sahip olmayan u_n kullanıcısının erişilebilirliği model üzerinden analiz edilirse işlem isteğiyle tetiklenen $T5$'in sonucunda yetki denetimi izin vermediğinden $T9$ tetiklenmeyecek ve işlem $P9$'da sonuçlanacaktır. Durum $[1101110001]$, başlangıç $[1000..0]$ ile M, $[00000000100..] = [1000.0] + [1101110001].I$ olur. Diğer işlemler, benzer sonuçlar ürettiği için burada sunulmamıştır. Analizin temel hedefi, yetki denetiminin, arşivde veya kurumlar arası yazışmalarda yetki kanıtı açısından yetersizliğinin incelenmesi üzerinedir. Analiz, takip eden kısımda iş akışında bir alım belgesinin onaylanması, arşivlenmesi ve kurumlar arası iletimi örneklenerek yapılmıştır.

Yetkili kullanıcı, u_a'nın bir alım belgesini onaylama işlemi iş akışında $\xrightarrow{t_7} M_{\mathrm{k}-1}$ $\xrightarrow{t_{11}} M_{\mathrm{k}}$ sonucunda kullanıcının belgeyi kendi anahtarıyla sayısal olarak imzalamasıyla gerçekleştirilir ve onaylı belge $d_a$oluşturulur.

İç saldırgan u_m 'nin iş akışında onaylı alım belgesi d_s oluşturma, yani bir alım belgesini oluşturma yetkisi olmadığı kabul edilsin. Bu yetki $T7$'de denetlenir ve u_m'nin erişilebilirliği $[000..001_{\{15\}}00..0] = [100..00] + [1101100..00]$ ile $\xrightarrow{t_7} M_{\mathrm{k}}$ ile $P15$'te sonlandırılır.

İç saldırganın yetki denetimini atlatarak d_s'$\mathrm{d_s}$yi oluşturup oluşturamayacağını inceleyelim. Kullanıcı u_m , alım belgesi oluşturma yetkisine sahip olsun, bu durumda $\xrightarrow{t_5} M_{\mathrm{k}-1} \xrightarrow{t_9} M_{\mathrm{k}}$, $P11$ ile d_c alım belgesini oluşturabilir. Daha sonra bu belgeyi iş akışı dışında kendi anahtarıyla imzalayıp aslında kurumsal yetki bakımından bir onay ifade etmeyen ama doğrulanabilir sayısal imzalı bir alım belgesi elde edebilir. Bu işlemi $\xrightarrow{t_{7^*}} M_{\mathrm{k}-1} \xrightarrow{t_{11^*}} M_{\mathrm{k}}$ ile P16 ve $P17^*$ şeklinde ve oluşan sahte onaylı belgeyi de d_s^* olarak ifade edelim.

u_m'nin arşive belge koyma veya kurumlar arası belge iletimi yetkisi olması durumunda, u_m d_s^* belgesi ile$\xrightarrow{t_4} M_{\mathrm{k}+1} \xrightarrow{t_8} M_{\mathrm{k}+2} \xrightarrow{t_{12}} M_{\mathrm{k}+3}$ ile $P21$ veya $\xrightarrow{t_4} M_{\mathrm{k}+1}$ $\xrightarrow{t_8} M_{\mathrm{k}+2} \xrightarrow{t_{14}} M_{\mathrm{k}+3}$ ile $P24$ yoluyla başarılı bir şekilde $P22$ ve $P25$'e erişebilecektir.

İlk durumun, yani u_m'nin sahte onaylı alım belgesi d_s^*'i arşive yerleştirmesinin yetki denetimi açısından analizi yapıldığında, eğer bir üst seviyede yetki denetimi

yoksa arşivde bulunan bir onaylı alım belgesinin gerçek onaylı belge olarak kabul edildiği görülmektedir. Belgede imzası bulunan kullanıcının onay yetkisi de kontrol edilmelidir. Çevrimiçi sorguda kullanıcının o an ki yetkileri kolayca sorgulanabilir. Oysa kurumsal iş akışında yetkiler dinamik bir yapıya sahiptir. Kullanıcılar zaman içinde atama, yetki düşürme, vekâlet gibi yetkinin genişlemesi veya azalması gibi dinamiklere tabi olurlar. Uzun süreli arşivlenen belgelerde kullanıcının -ki artık kullanıcı sistem dışı dahi olabilir- o an ki yetkileriyle belgenin geçerliliğinin yani işlem yapıldığındaki yetkilerinin tespiti mümkün olmayacaktır.

Örneğin u_m, belirli bir zaman aralığında u_a ya vekâlet etmiş olsun. O zaman zarfında sahip olduğu onay yetkisi, iş akışında $\xrightarrow{t_7} M_{\mathrm{k}-1} \xrightarrow{t_{11}} M_{\mathrm{k}}, P17$ ile geçerli bir onay belgesi oluşturmasına izin verir. Yetki denetimi, bu belgenin arşive gönderilmesi sonucu oluşan gerçek onaylı d_s ile yetkisizken oluşturduğu d_s^*'yi ayırt edebilecek bir mekanizmaya, her iki belge için geçerlilik kararına etki edebilecek doğrudan bir yetki kanıtına sahip değildir. Çözüm olarak ilk akla gelen yöntem olan işlem günlüklerinin kullanımı, bu tür yetki doğrulamalarında dolaylı ve uzun süreli saklanan arşiv belgeleri için zor bir seçenek olacaktır.

Kurumlar arası yazışmalarda, onaylı bir alım belgesinin geçerliliğinde yetki denetiminin cevabı benzer şekilde yetersiz kalmaktadır. İş akışı dışında kalmış saldırgan v'nin bir alım belgesi oluşturup bunu A kurumundan geliyormuş gibi B kurumuna ilettiği bir senaryo oluşturalım. v iş akışı dışında bir d_o^* belgesi oluşturur ve bu belgeyi kendi anahtarıyla imzalayarak sahte onaylı bir d_s^* alım belgesi üretir. Bu belgeyi B kurumuna iletir. B kurumu d_s^* üzerindeki imzayı doğrular ama yetki denetiminin ikinci aşaması olarak v'nin A kurumuyla ilişkisini de kontrol eder. v, A kurumunda çalışmıyor veya yetkili değilse d_s^*'yi geçersiz olarak kabul edilir. Bu kontrol kimlik denetimi ile gerçekleştirilir. Bir anlamda v'nin iş akışında $[T0, T1, T2]$ tetiklemesini yaparak $P4$'e dâhil olup olmadığı kontrol edilir.

A kurumundaki kullanıcılar söz konusu olduğunda onaylı alım belgesinin B kurumundaki yetki kontrolündeki karşılığı önemlidir. Yetkili kullanıcı u_a'nın iş akışında $\xrightarrow{t_7} M_{\mathrm{j}-1} \xrightarrow{t_{11}} M_{\mathrm{j}}, P17$ sonucunda hazırladığı yetkili d_s ile saldırgan u_m'nin $\xrightarrow{t_5} M_{\mathrm{j}-1} \xrightarrow{t_9} M_{\mathrm{j}}, P11$ den ve $\xrightarrow{t_{7^*}} M_{\mathrm{k}-1} \xrightarrow{t_{11^*}} M_{\mathrm{k}}$ ile $P16^*, P17^*$ geçiş dizisini kullanarak ürettiği d_s^* arasında bir fark yoktur. Çünkü onaylı alım belgesi, onaylayanın kimliğini kanıtlayan ve belge bütünlüğünü destekleyen sayısal imza dışında bir denetim verisi

içermemektedir. Hem u_a hem de u_m kimlik denetiminden geçebildiği için A kurumunda belge üretebilir durumdadır. B kurumu d_s veya d_s^*'i doğrudan kabul edebilir veya A kurumu ile iletişime geçip d_s^*'in geçerliliğini onaylatabilir. B'nin yetki denetimi kapsamında A ile yaptığı bu yazışmaların ilgili dokümana ait bir yetki kanıtı olması için dokümanla birlikte saklanması gerekir. Bu A'nın dokümanı reddedememesinin garantisidir.

Yapılan analizin sonuçları iş akışında durum ve olaylar karşısında saldırganlar ve yetkili kullanıcının gerçekleme başarılarını ve yetki denetim özelliklerini gösterecek şekilde Tablo 3.3'de özetlenmiştir. Tabloda yetki zaafiyetleri kalın harflerle vurgulanmakta, gölgeli satırlar ise çözüm için ipuçları taşımaktadır. Denetim olmadığı durumda iş akışında tüm işlemler yetkisiz gerçekleştirilmekte (Tablo 3.3- 1.a, 5.a), kimlik denetimi ile dış saldırgan engellenmektedir (Tablo3.3-1.b, 2-a, 5-b). İşlem yetkilerinin varlığında (Tablo 3.3- 2.b, 3.b, 4, 6) kullanıcıların yetkileri dâhilinde işlem yapmaları sağlanmaktadır.

Arşiv ve kurumlar arası yazışmalar gibi süreçler iş akışında yetki denetiminin kapsamı dışında kalabilmektedir. Bu durum, denetimde zafiyete sebep olmaktadır. Yapılan analiz sonucunda aşağıdaki çıkarımlar elde edilmiştir.

- Arşivlenmiş belgeler, kurumsal yetki ile ilişkilendirilmediklerinden üzerlerinde yetki denetimi kapsamında bir geçerlilik kontrolü yapılamamaktadır. Bu durum, arşivdeki belgelerin güvenilirliklerine şüphe düşürmektedir.
- Erişilebilirlik analizi ile iç saldırganın, oluşturduğu sahte yetkili bir belgeyi arşivleme ve/veya kurumsal yazışma işlemlerini gerçekleme yetkilerini kullanarak yetki denetiminden geçmiş geçerli bir belge gibi sürece dahil edebildiği ortaya konulmuştur.
- Kurumlar, kimlik doğrulama ile saldırganın kaynak kurum kullanıcısı olmadığını ayırt ederek belgenin yetki denetimini sınırlı şekilde yapabilmektedir.
- Kurumlar arası yazışmalarda, yetki taşınmamakta kurumsal yetki denetlenmemektedir.
- Kurumsal yetkilerin, politikalar ve yönergelere uygun olarak gerekli detaylara sahip olacak şekilde tanımlanması ve iş akışına bu şekilde yansıması gereklidir. Bu eksiklik yetki denetiminde kontrolün istenen seviyede yapılamamasına sebep olmaktadır.

• Yetkiler, yetki denetiminin sürdürülebilirliği ve etkinliği açısından, iş akışı sürecinde belirtilen noktalarda kontrol ve ispat imkanı sağlanması açısından erişilebilir olmalıdır. Ancak bu şekilde, yetki denetimi, iş akışındaki belgelerin, yetkiler dahilinde üretildiğinin belirlenmesi ve doğrulanabilmesini tam olarak sağlayacaktır.

Tablo 3.3: Yapılan analizin sonuçları

Olaylar	Durumlar	Gerçekleme			Yetki Kanıtı	Yetki Denetim Kapsamı
		DS	İS	YK		
1. Kurumsal iş akışında herhangi bir işlem gerçekleştirme ($T4$) ve ($T9, T10, T13, T15$)	a. Hiç yetki denetimi yok ($T0, T5, T6, T7, T12, T14$ tetiklemelerin olmadığı durum) ($P4$)ve ($P11, P14, P17, P22,25$)	**2**	**2**	2	Yok	Yok
	b. Sadece Kimlik denetimi var ($T5, T6, T7, T12, T14$ tetiklemelerin olmadığı durum) ($P2$), ($P4$) ve ($P11, P14, P17, P22,25$)	0	**2**	2	Kullanıcı kimlikleri	Kullanıcı
2. Kurumsal iş akışında yetkili bir işlem gerçekleştirme ($T1$) ve ($T5, T6, T7, T12, T14$)	a. Sadece Kimlik denetimi var ($T5, T6, T7, T12, T14$ tetiklemelerin olmadığı durum) ($P2$), ($P4$) ve ($P11, P14, P17, P22, 25$)	0	**2**	2	Yok	Kullanıcı
	b. Yetki denetimi var ($P2$), ($P4$) ve ($P11, P14, P17, P22,25$)	*0*	*1*	*1*	Atanmış işlem yetkisi	İşlemler
3. Arşivde belge oluşturma ($T8$) ve ($T12$)	a. Kullanıcıların arşivleme yetkisi yok ($P18$) ve ($P20$)	0	0	0	Kullanıcıların işlem yetkileri	İşlemler
	b. Kullanıcıların arşivleme yetkisi var ($P18$) ve($P21, P22$)	0	**2**	2	İşlem yetkisi	İşlemler
4. Arşivde yetkisiz belge oluşturma ($T8$)	Kullanıcıların arşivleme yetkisi var ($P18$) ve($P21, P22$)	0	**2**	2	İşlem yetkisi var	İşlemler
5. Kurumlar arası belge iletimi ($T8$)	a. Kurumlar arası kimlik denetimi yok ($P19$)ve ($P25$)	**2**	**2**	2	Yok	Yok
	b. Kurumlar arası kullanıcı kimlik denetimi var ($P19$)ve ($P25$)	0	**2**	2	Kullanıcı kimlik	Kurumdaki kullanıcı
6. Kurumlar arası yetkili belge iletimi ($T14$)	Kurumlar arası kimlik denetimi var ($P19$) ve ($P25$)	0	**2**	2	Kullanıcı kimlik	Kurumdaki kullanıcı
Önerilen durum 1: işlem yetkisinin taşınabilirliği ve doğrulanabilirliği	Kurumlar arası **yetki denetimi** var ($P19$) , ($P23, P24$) ve ($P25$)	0	*1*	*1*	İşlem yetkisi	Kurumdaki işlem yetkili kullanıcı
Önerilen durum 2: kurumsal yetkinin doğrulanabilirliği	Kurumlar arası **kurumsal yetki denetimi** var ($P19$), ($P23, P24$) ve ($P25$)	*0*	*1*	*1*	Kurumsal yetki	Kurumdaki yetkili kullanıcı

(Başarı ölçütleri: 0: hiçbir, 1:bazı, 2:tüm işlemler; DS:Dış Saldırgan, İS: İç Saldırgan, YK: Yetkili Kullanıcı)

Analiz ve çıkarımlarda vurgulandığı gibi yetkilendirme uygulama eksiklikleri yetki denetiminin kurumsal iş akışında görevini tam olarak yerine getirmediğini ortaya koymaktadır.

3.3. Modelin Mekanizması

Önceki bölümde, her bir katmanındaki yetki denetim mekanizmaları ve bu katmanların Petri ağları ile bir kullanıcı üzerinden erişilebilirliği tanımlanmıştır. Bu bölümde çok katmanlı yetki denetim modeli özellikleri ile incelenmektedir.

U, G, O, R, A sırasıyla kullanıcılar, kullanıcı grupları, işlemler, roller ve yetkiler kümeleri olarak tanımlansın. Öyle ki her kullanıcı, bir grubun üyesi olsun: $\forall u \in g, u \in U$ve $g \in G$. Roller kullanıcı grupları için tanımlanmış işlemler olmak zere her işlem için en az bir rol tanımlı olsun. Rollerin tanımı denklem (3.1)'de sunulmaktadır.

$$r: g \to o, \exists r \forall o \in O,\ r \in R, g \in G. \tag{3.1}$$

Yetkiler kullanıcıların roller olmak üzere yetki a denklem (3.2)'de tanımlanmaktadır.

$$a = \{\{u, r, o\} | u \in g \wedge r: o \to g\}, r \in R, g \in G, a \in A. \tag{3.2}$$

Yetki onayı y ise denklem (3.3)'teki gibidir:

$$y = \exists a \left\{ a \in A \middle| a = \{\{u, r, o\} | u \in g \wedge r: o \to g\} \right\} \to \{0,1\}. \tag{3.3}$$

Eğer bir kullanıcının işlem üzerinde tanımlı bir rolü varsa yetki onaylanır. Aksi durumda reddedilir. Eğer $u \in g$ ise grup g için yetki onayı denklem (3.4)'deki gibi gerçekleşir.

$$y = r: o \to u, \text{ öyle ki } u \in g. \tag{3.4}$$

Yetki denetim katmanları yetkinin kapsamına göre organize edilmiştir. İlk katman, sistem oturum açma katmanıdır. Yetki denetimi tüm kullanıcı kümesi U üzerinde etkindir. Bu katmanda kullanıcılar, $g_0, g_x \in G$ olmak üzere; sistem tarafından bilinen(g_0) ve tanımsız(g_x) kullanıcılar olarak gruplanabilir, İşlem tanımı $o_0 \in O$ modeldeki en geniş tanım olan sistem erişimi olarak tanımlanmaktadır. Kullanıcının yetki denetimindeki rolü $r_0: g \to o$ ile sistem genelinde onay veya ret olacaktır. İlk

katmanda kullanıcının tanımlanması ve grubunun belirlenmesi kimlik doğrulama mekanizmaları ile sağlanır. $r: o \rightarrow g$ ifadesi, kimlik tanımlayıcının (ID) $u \in g_0$ kapsamındaki tanımıdır.

Bu katmandaki yetki tanımı denklem (3.5)'de verilmiştir:

$$a_0 = \{\{u, r, o\} | u \in g_0 \wedge r: o_0 \rightarrow g_0\} \quad (3.5)$$

Kullanıcı $y = 1$ onayı ile sistem erişimi doğrulanır. Eğer sistemde sadece ilk katman bulunuyorsa, kullanıcı u , sistemde her işlemi $(\forall o \in O)$ gerçekleyebilir. Eğer $u \in g_0$ ise $\{r: o \rightarrow g\} \rightarrow \{1\}$ ve $y = 1$ dir. $u \in g_0$ bu yetki denetimi sonucunda sistem genelinde yetkili olacaktır. Eğer, $u \in g_x$, ise $\{r: o \rightarrow g\} \rightarrow \{0\}$ ve $y = 0$ dır. Yetkisiz erişim reddedilir.

Yetki denetiminin ikinci katmanında, kullanıcı grupları üzerinde erişim kontrolü uygulanır. Bu katmanda yetki denetimi erişim listeleri ile sağlanır. Yetki denetimi önceki katmanda filtrelenen kullanıcılara $u \in g_0$ ve $g_0 \subset U$ uygulanır. İşlemler listelerde tanımlanır, öyle ki $O_{ACL} \subseteq O$'dır. Kullanıcı grup ve roller de listede tanımlıdır. $o_{ACL_1} \in O_{ACL}$, $g \in G$, olmak üzere $r: o \rightarrow g$ $r: o_{ACL_1} X\ g$ olarak tanımlanır. Yetki bilgisi, $r: o_{ACL_1} X\ g$ kısıtlaması ile güncellenmiştir. Eğer $r: oXg$ listede tanımlanmışsa işlem o , $o \in O_{ACL}$için yetki onayı verilir.

Sistem gereksinimlerini bir yana koyduğumuzda her bir {işlem, grup} ikilisini listede tanımlamak zordur. Bu durumda yönetim zorluğu da açıkça artacaktır.

Üçüncü katman, ikincisinde karşılık bulmayan yetki denetim gereksinimleri için bir mekanizma sunmaktadır. İşlemler için yetkiler rol tabanlı yaklaşımla daha detaylı tanımlanmaktadır. Kullanıcı ve gruplar da rollerle daha kolay yönetilmektedir. Kullanıcılar gruplar üzerinden yetkilendirilir. Bu katmanın kapsamındaki kullanıcı grubu ikinci katmandan farklı değildir. İkinci katmanda kısıtlamalar,$O_{ACL} X\ G$ üzerinde tanımlanmaktayken, üçüncü katmanda roller $R: O \rightarrow G$ şeklinde daha geniş kapsamlı olarak tanımlanır. İkinci katmanda yetkinin yükseltilmesi gibi bir değişiklik, listelerde güncelleme gerektirmekteydi.

Rol tabanlı yaklaşımda vekâlet mekanizması yer alır[30]. Görevlerin ayrılığı (SoD)[31] ilkesi geniş kapsamlı rol tanımının ortaya çıkarabileceği istenmeyen durumlar için her kullanıcının ilişkili işlemler için sadece tek bir rolü olması gerekmesi belirlenmiştir. Kurumsal işlemlerin güvenliği için bu yaklaşım önemlidir. Satın alma

yetkisine sahip biri asla satın alma onay rolüne hiçbir zaman sahip olmamalıdır. Bu değişmez kural, kişinin hem satın alma hem de satın alma onayı rollerine sahip olabileceği ama onay yetkisinin kendi alımında kullanamayacağı şeklinde dinamik olarak uyarlanabilir. Bu katmandaki yetki, denklem (3.6)'da tanımlanmaktadır:

$$a = \{\{u, r, o\} | u \in g \wedge r: o \rightarrow g\} \tag{3.6}$$

$\{o_t, o_h\}$ iş akışında iki bağımlı işlem olsun. rol $r, r_t : o_t \rightarrow u \wedge \nexists r_h : o_h \rightarrow u$ kuralı ile sınırlıdır. Bu katmandaki yetki onayı denklem (3.7)'de sunulmaktadır:

$$y = \exists a \left\{ a \in A \middle| a = \{\{u, r, o\} | u \in g \wedge r: o \rightarrow g\} \right\} \rightarrow \{0,1\}. \tag{3.7}$$

Bu durumda, yetki vekâleti kapsamındaki onay ise, $y_{uu'}$, kullanıcı u'den kullanıcı u'ya vekaleten aktarılmış yetki bilgisi olmak üzere denklem (3.8)'de ki gibidir:

$$y^u = \exists a \left\{ a \in A \middle| a = \{\{u, r, o\} | u \in g \wedge r: o \rightarrow g\} \right\} \wedge y_{uu'} \rightarrow \{0,1\} \tag{3.8}$$

Bu bilginin doğrulanması işlem o için yetkilendirme sağlar. Satın alma durumunun üçüncü katmanda tanımlanması aşağıdaki gibidir. o_p satın alma işlemi ve g_p satın alma grubu olmak üzere; satın alma rolü $r_p: o_p \rightarrow g_p$ şeklinde tanımlansın. Denklem (3.9) da verilen yetki onayı geçerli olacaktır.

$$y = \exists a_p \left\{ a_p \in A \middle| a_p = \left\{ \{u, r_p, o_p\} \middle| u \in g_p \wedge r_p: o_p \rightarrow g_p \right\} \right\} \rightarrow \{0,1\} \tag{3.9}$$

Rol tabanlı yaklaşım her ne kadar ikinci katmandaki zayıflıkları çözümlese de örnek durum üzerinden verilebilecek "eğer satın alma işlemi …TL değerinden yüksekse satın alma onayı yetkisi birim başkanına aittir." gibi kurumsal yönerge ve rehberlerde yer alan ifadelere karşılık verememektedir. Yetkiler, atomik işlemlere tanımlanmış olsa da kısıtlamalar ve istisnai özel durumlar rollere dâhil edilmemektedir. Rol tanımları, yetki denetiminin kurumsal iş akışında tam olarak yerine getirilmesi için yönerge ve politikalarda yer alan işlem ve grup tanımlamaları

gibi kısıtlamaları da içermelidir. D, yönergede tanımlı durumlar kümesi olmak üzere, $d \in D$ ve d^r r rolü için tanımlı bir durum olsun. Yetki denklem (3.10)' de verildiği gibi genişler:

$$a_p = \left\{ \{u, r_p, o_p, d_p\} \middle| u \in g_p \wedge r_p : o_p \rightarrow g_p \wedge o_p \subset {d_p}^{r_p} \right\} \quad (3.10)$$

Bu tanımda o_p işlemi için yönergede tanımlanan kısıtlama yetki tanımına dâhil edilmelidir. Yetki denetimi denklem (3.11)'te gösterildiği gibi güncellenir.

$$y = \exists a_p \left\{ a_p = \left\{ \{u, r_p, o_p, d_p\} \middle| u \in g_p \wedge r_p : o_p \rightarrow g_p \wedge o_p \subset {d_p}^{r_p} \right\} \right\} \rightarrow \{0,1\} \quad (3.11)$$

Kurumsal yönergeleri işlem kümesinde özel işlemler olarak tanımlamanın birçok yönetimsel avantajı vardır. Aynı işlemler için farklı roller için iş akışında farklı süreçlerin tanımlanması iş akışını hızlandırsa da karmaşıklaştırır. Yönergeler, politikalar ve kurumsal işlevler sistemde zaman içinde değişme ve güncellenme eğilimindedirler. Eğer iş akışında tanımlamak yerine işlem kümesinde tanımlama yapılırsa işlemler daha hızlı güncellenerek sisteme otomatik olarak uyumlu hale geleceklerdir. Çok katmanlı modelin dördüncü katmanı kurumsal yetki tanımlarının önerildiği yetki denetim mekanizmasını kapsamaktadır.

- Çok Katmanlı Yetki Denetim Modelinin Dördüncü Katmanı

Üçüncü katmanda yer alan rol tabanlı mekanizma, işlemler üzerinde detaylı denetim sağlamasına rağmen hiçbir rol tabanlı modelin kurumsal yönerge ve politikaları roller üzerinde uygulayamadığı bilinmektedir. Rol tabanlı mekanizmalarda SoD kısıtlamaları belgeler üzerindeki hassas işlemler için güvenlik mekanizması olarak yer alsa da bu yöntemin kurumlar arası yazışmalarda farklı rol tanımları ve kısıtlamalar ile rol atama problemleri oluşturduğu görülmüştür [31].

Bu tezde önerilen dördüncü katmanda yetki denetiminin yönergeleri de içermesi sağlanmaktadır. Karar mekanizması yönergelerdeki yetki kısıtlarını göz önünde bulundurarak kullanıcıyı yetkilendirmektedir. Bu mekanizma, belgelerin güvenilirliğinin önemli olduğu durumlara da uygulanabilir. Çünkü bu katmanda yer

alan mekanizma, belgenin yetkili biri tarafından sağlandığına dair güçlü kanıtlar sunmaktadır.

Belgenin güvenilirliği ile ilgili örnek durumu, satın alma onayı üzerinden açıklayalım. Kullanıcı u_m önceki bölümde olduğu gibi satın alma belgesini oluşturabilir. Kullanıcı u_a nın onay rolünü kısa bir süreliğine kullanıcı u_m 'ye devrettiğini düşünelim. Bu durumda kullanıcı u_m satın alma belgesini onay için imzalayabilecektir. Oluşturulurken imzalanan alım belgesi ile onay için imzalanan satın alma onay belgesi üzerindeki yetki farkı belirsizdir. Her iki belgede sistemde tanımlı birimler tarafından gerçekleştirilmiştir. Fakat belgelerden ikisi de bir yetki bilgisi içermemektedir. Öyle ki kullanıcı u_m kendisi adına mı yoksa vekalet ettiği birim başkanı rolü ile mi onaylamıştır bilgisi yoktur.

Sayısal imza işlemi zamanpulu mekanizmasına sahiptir ve vekalet de sistemde sadece kısa bir süre kullanılabilmektedir. Bu iki ayrık bilginin sorgulanması özellikle kurumlar arası kayıtlar ve uzun ömürlü dokümanlar için zordur. Bununla birlikte kurumlar arası yazışmalarda, kurumsal rollerin ve zamana bağlı özniteliklerin paylaşılması güvenli değildir. Bu durumda da diğer kuruluşun yetkileri sorgulama ve değerlendirme olanağı bulunmamaktadır.

Bir belgenin oluşturulması veya bir işlemin gerçekleştirilmesinde yetkinin doğrulanması iş akışında aktif olan yetkilendirmeler ile mümkün olmaktadır. Yetki denetimine söz konusu olan nesne ve yetkinin kapsamı anlık gerçekleştirilebilmektedir. Ama iş akışı dinamik yapıdadır ve bu yapı yetki denetiminde önceden var olmuş nesne ve kapsamların elde edilmesini zorlaştırmaktadır. Anlaşmalar, mali kayıtlar ve hasta dosyaları gibi uzun süre saklanan belgelerde yetkinin kontrolüne dair kanıt elde edilmesi zorlaşmaktadır [38], [39]. Bu belgeler üzerinde gerçekleştirilmiş sözleşme ve hasta geçmişine ait bilgiler gibi çoklu işlemler ay ila yıllar gibi farklı aralıklarda gerçekleşmiş olabilmektedir. Bu geçen sürede yetkinin değişimi iş akışının dinamik yapısında normaldir.

Önceki katmanların yetki denetimine odaklanmasının yanında, dördüncü katman işlevleri arasında, yetkinin doğrulanmasını da kapsar. Bu mekanizma için ilgili yetki bilgisi işlemlere eklenmektedir. Doğrulama, bu bilgi üzerinden gerçekleştirilir. Hedeflenen doğrulama, sadece anlık değil; geçmişe dönük, uzun süreli saklanan belgelerde de yetki doğrulamanın yapılabilmesidir. Bu özelliği ile belgelerin güvenilirliğini destekler.

İkinci katmanın izin ve gerçekleştirme noktalarıyla üçüncü katmandaki kontrol

ve gerçekleştirme noktalarında farklılık gözlemlenmektedir. Her iki gerçekleştirme işlemi, iş akışında, kurumsal yönerge veya politikalar doğrultusunda onay veya ret ile sonlanmaktadır. Sistem ağ üzerinde $P4$ve $P7$ de sonlanmakatadır.

Kimliği doğrulanmış kullanıcı u_{id}, $[t_0\, t_5\, t_7\, t_8\,]$:$[100001011]$'I tetikleyebilir. $[10000000]$ ilk işaretiyle erişilebilirlik $[0000001] = [10000000] + [100001011] \cdot I$ olmaktadır. Kullanıcı u_{id}, yer p_7'ye $M_0 \xrightarrow{t_0} M_2 \xrightarrow{t_5} M_3 \xrightarrow{t_7} M_4 \xrightarrow{t_8} M_5$ $\{p_0, p_1, p_5, p_6, p_7\}$ üzerinden erişir. Yer p_7'de kullanıcı u_{id}, eğer u_{id}'nin r rolünün gerçekleme izni varsa, yönergede tanımlı olan ${d_p}^{r_p}$ ile o_i işlemini gerçekleyebilir. Bu katmandaki yetki onayı denklem (3.12)'de sunulmaktadır:

$$y = \exists a_p \left\{ a_p \; = \left\{ \{u, r_p, o_p, d_p\} \middle| u \in g_p \wedge r_p : o_p \rightarrow g_p \wedge o_p \subset {d_p}^{r_p} \right\} \right\} \rightarrow \{1\} \quad (3.12)$$

4. VAKA ÇALIŞMASI ve ANALİZLER

Bu bölümde, tez çalışmasında gerçekleştirilen vaka çalışması ve ilgili analizler yer almaktadır.

4.1. Kurumsal İş Akışında Yetki Denetiminin Sürdürülebilirliği İçin Bir Vaka Çalışması: Yetkili Sayısal İmza Modeli

Önerilen yetkili sayısal imza çözümü ile imzaya yetki eklenerek yetkilendirme taşınabilir hale getirilmekte ve bu ek bilgi ile imzalı belgede yetki tespiti gerçekleştirilmektedir.

Literatürde imza yetkilendirme üzerine vekil imzalar [17] veya grup imzalar [18], [19] kapsamında birçok çalışma yayınlanmıştır. Bu çalışmalar, bir grup veya birimin, başka bir birim adına imzalama hakkına sahip olabildiği yaklaşımlar sunmuşlardır.

Literatürde sayısal imzaya bilgi eklenmesi üzerine yaklaşım örnekleri de bulunmaktadır. Kendinden sertifikalı ve kimlik tabanlı imza yöntemleri [20], [21] imza anahtarı oluşturulmasına farklı bir açıyla yaklaşan ve imzayı, imzalayana ait bir bilgi ile oluşturma yoluna giden yöntemlerdendir.

İmzalı belgelerde yetki konusu, kurumlarda, kurum politikaları, yönetmelik ve yönergelerle belirlenmiştir. Bahsi geçen imza yaklaşımlarının hiçbiri, kurumsal yönerge ve politikaların sayısal imzaya eklenerek kurumsal bir yetki kanıtı oluşturacak şekilde kullanılması gibi bir çözüm getirmemektedir.

Kurumsal belgedeki imza yetkisi denetimi, ancak, belgeyi imzalayan kişinin kimliğinin doğrulanması, belgenin bütünlüğünün korunmuş olması, imzalayanın belgenin geçerliliğini gerektiren yetkiyi taşıması ve doğrulama sırasında ilgili yetkinin belgelenebilmesi durumları sağlandığında süreklilik arz eder.

Önerilen yetkili sayısal imza şemasında; İmzalayan i, belge M'yi, kendi gizli anahtarı PR_i ve yetki bilgisi A'yı kullanarak oluşturduğu yetkili imza anahtarı PR_{iA} ile imzalar. Doğrulayan, i'nin açık anahtarı PU_i (kullanılan şema açık anahtarın güncellenmesini gerektirmemektedir) ve A ile imza ve kurumsal yetkiyi doğrulayabilir. Yetki denetimi işlevinin imzaya kazandırıldığı model, imza ile yetki

bilgisini birleştirerek, yetkili sayısal imzayı üretme, gerçekleştirme ve doğrulama işlevlerini içerir.

Yetki kanıtının, kurum ve süreç dışına taşınabilmesine olanak sağlayan veri "yetki bilgisi" şeklinde adlandırılmıştır. Bu yapı, temelde kurumsal yetki politikaları ve imza yönergelerinde tanımlanan, yetki konusunu, yetkinin geçerlilik zamanını ve yetkili kimse hakkında bilgi içeren bir sertifika yapısıdır. Kimlik denetimi için kullanılan sertifikalar, yetki tanımı ile genişletilerek kullanılan sistemlere uyumluluk sağlanabilir. Şekil 4.1'de X.509 kimlik[40] ve Şekil 4.2'de öznitelik sertifikalarının[41] Yetki makamı (YM), Yetki Geçerlilik Aralığı (T-Ai), Yetki Tanımı (Ai) ifadeleri ile genişletilmesiyle elde edilen yetki bilgisi sertifika yapıları sunulmuştur.

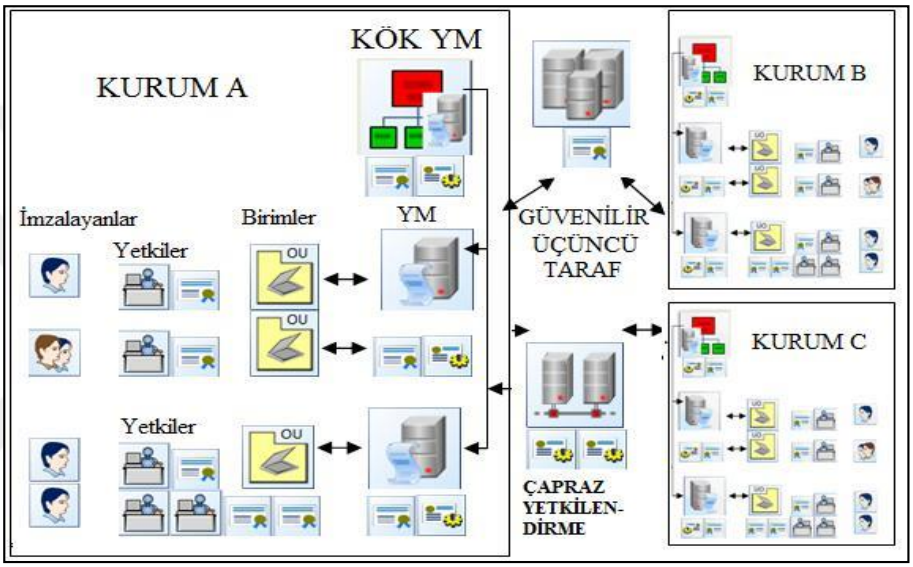
Yetkili sayısal imza, var olan sistemlere uyumluluk göstermesi, kriptografik ve sistem gereksinimlerinden dolayı Açık Anahtar Altyapısı [42] üzerine kurulmuştur. YM'nin modeldeki yeri ve fonksiyonu Şekil 4.3'de gösterilmiştir. YM temel olarak sertifika yaşam döngüsü görevlerini yetki bilgisi kapsamında üstlenir.

X.509	*X.509 yetkibilgisi yapısı*
Sürüm	**X.509 ile aynı**
Sertifika seri no	**X.509 ile aynı**
İmza algoritması tanımlayıcı	**X.509 ile aynı**
Algoritma	
Parametre	
Yayımlayıcı	**Yetki Makamı**
Geçerlilik	**T-A_i**
Başlangıç	
Son	
Konu	**i**
Konu Açık Anahtar Bilgisi	**X.509 ile aynı**
Algoritmalar	
Parametreler	
Açık Anahtar	**PU_i**
Yayımlayıcı benzersiz tanımlayıcı	**YM veya PU_{YM}**
Konu benzersiz tanımlayıcı	**ID_i**
Genişlemeler	**A_i**
	T_A
İmza	**S**
Algoritma	**X.509 ile aynı**
Parametreler	
Şifreli	

Şekil 4.1: Yetki bilgisi X.509 Sertifika Yapısı

X509 Öznitelik Sertifikası RFC3281	*Yetkibilgisi yapısı*
Öznitelik Sertifikası	**Yetkibilgisi**
Öznitelik Yetkilisi	**YM**
Yayımlayıcı	**Yetki Makamı**
Sahibi	**PU_i**
Öznitelik	**A_i**
Geçerlilik Aralığı	**$T\text{-}A_i$**
imzaDeğeri	**S**
Genişlemeler	**T_A**

Şekil 4.2: Yetki bilgisi Öznitelik Sertifika Yapısı



Şekil 4.3: Modelde Yetkilendirme Makamı

Eşleme tabanlı kriptografinin altındaki temel fikir, iki kullanışlı kriptografik grup arasında problemler arası indirgemeye dayanan ve yeni kriptografik şemalar oluşturmaya izin verebilecek bir denklik ilişkisi inşa etmektir. Öyle ki, asal q dereceli G_1ve G_2 grupları bulunsun. P ve Q, G_1'e ait iki üreteç olmak üzere eşleme e: $G_1 X\ G_1 -> G_2$ şeklinde tanımlanır ve

- Çift doğrusallık: $P, Q \in G_1$ ve $a, b \in Z_q$ olmak üzere $e(aP, bQ) = e(P, Q)^{ab}$,
- Dejenere olmama: $P \in G_1$ öyle ki $P \neq 0$ ise $e(P, P) \neq 1$,
- Hesaplanabilirlik: e verimli şekilde hesaplanabilir,

özelliklerine sahiptir.

Bu özellikleri taşıyan Tate ve Weil eşlemeleri, anahtar paylaşımı [43], kimlik tabanlı şifreleme, sayısal imza [36], [37] gibi birçok şemada kullanılmış ve eşleme tabanlı kriptografi kavramını oluşturmuştur.

Önerilen şemanın kayıt, üretim ve doğrulama evreleri aşağıdaki gibidir.

Kayıt sürecinde, yetki bilgisi YM'de oluşturulur, onaylanır ve imza için kullanılmak üzere imzalayana gönderilir. İmzalayan taraf, aynı yetki için YM'ye yetki bilgisinin geçerlilik süresi bitmediği sürece, tekrar yetki bilgisi oluşturmak için başvurmaz ve üretilen yetki bilgisi ile yetkili imza anahtarını oluşturur. Yetkili imza anahtarı, (4.1)'de tanımlanan g üreteç ve PR_i gizli anahtar parametre değerlerinden (4.2)'de tanımlanan işlemler sonucunda elde edilmektedir.

$$g \in G, e(g,g) \neq 1;\ PR_i \in Z_q^* \tag{4.1}$$

$$PU_i = PR_i.g\ ve\ PR_{iA} = PR_i.H1(A) \tag{4.2}$$

Yetkili sayısal imza, kayıt sürecinde elde edilen yetkili imza anahtarı PR_{iA}, belge (ileti) M ve bu evrede üretilen tek kullanımlık rastgele seçilmiş imza oturum değeri n, yardımıyla önerilen eşleme tabanlı imza şemasıyla oluşturulur. İmza, (S,R), (4.3) kullanılarak üretilir.

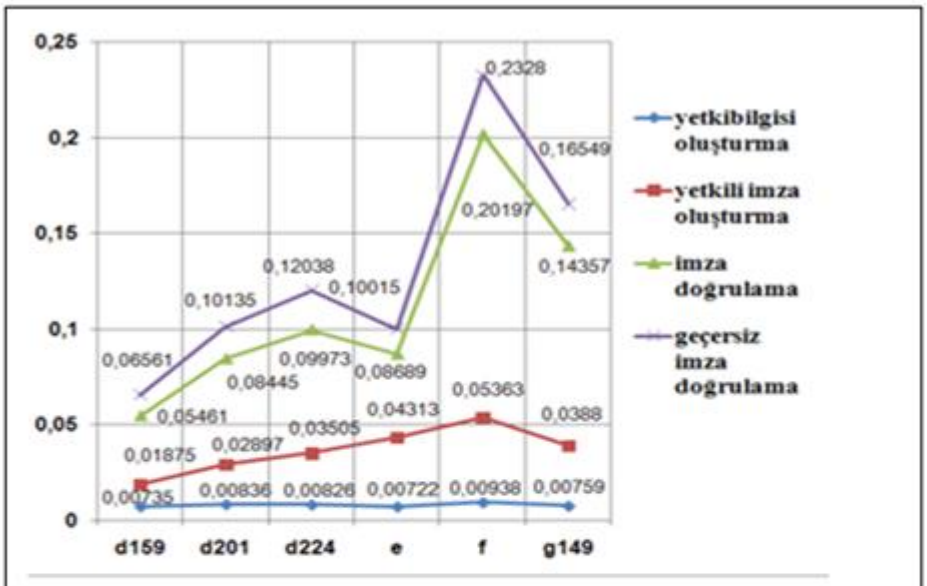
$$R = n.H1(A), r = H2(M,R) \text{ ve } S = (n+r).PR_{iA} \tag{4.3}$$

Doğrulama sürecinde yetki bilgisi ve yetkili sayısal imza doğrulanır. Doğrulayan taraf öncelikle imzayı açık anahtar ile doğrular. YM'ye yetkibilgisinin doğrulanması isteğini gönderir. YM'de yetkibilgisi ve ilişkili yetki konusunu kontrol edilir. Doğrulayan taraf YM'den aldığı onay cevabına göre imzayı kabul veya reddeder. İmzanın doğrulanması, kriptografik çift doğrusal eşleme özellikleri ile elde edilir. Eğer denklem (4.4) sağlanıyor ve YM, yetkibilgisini doğrulamışsa yetkili imza doğru ve geçerlidir.

$$e(g,S) = e(PU_i, R + r.H1(A)) \tag{4.4}$$

4.2. Gerçekleme ve Performans Analizi

Önerilen yetkili sayısal imzalama modeli, Ubuntu 10.04 işletim sistemi üzerinde, açık kaynak kodlu eşleme tabanlı kriptografi ve GMP matematiksel tanım kütüphaneleri [44], [45] kullanılarak gerçeklenmiş ve yapılan performans/güvenlik analizleri verilmiştir. Gerçeklemenin farklı eşleme tipleri üzerinden elde edilen yetkili sayısal imza uygulamasının aşamalarına ait performans karşılaştırma grafiği eşleme özellikleri ile Şekil 4.4'de sunulmuştur.



Tip	Alan büyüklüğü	k-eğri derecesi	Dlog güvenlik	Eğri elde yöntemi
dn	n	6	6n	MNT
e	1024	1	1024	CM
f	160	12	1920	Paulo-Barreto.
gn	n	10	10n	Freeman-Scott

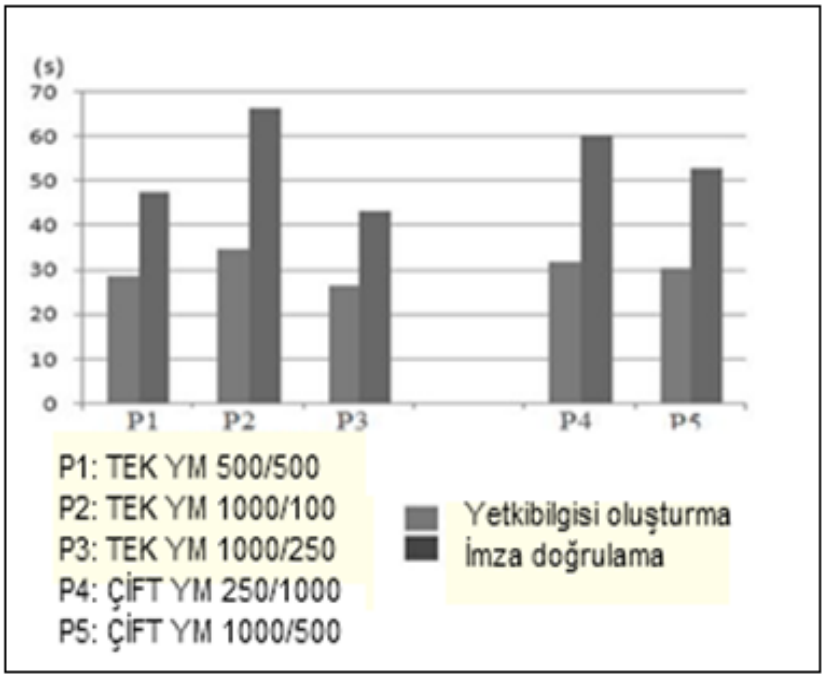
Şekil 4.4: Yetkili sayısal imzanın farklı eğri tipleriyle gerçeklenme performans grafiği

Yetki bilgisi oluşturma zamanının farklı eşleme tiplerinde çok az değiştiği görülmekte olup sisteme fazla yük getirmeyeceği ve şemada, imzalayan için performans belirleyici işlemin doğrulama olarak öne çıktığı görülmektedir. Yetkili imza oluşturma ve doğrulama işlem süreleri göz önünde bulundurulduğunda, d159'un

en kısa, f tipi eşlemenin ise en uzun sürede sonuçlandığı görülmektedir. Ortalama 0,04ms sürede gerçekleştirilen imzalama işlemi, tüm tiplerde işlem yoğunluğuna sahip sistemler için uygun özellik göstermektedir.

Yapılan diğer performans analizi ile YM üzerindeki yük incelenmiştir. YM'nin yetki bilgisini üretmesi ve imza doğrulama görevlerini, eş zamanlı çoklu istemcilerden gelen istekler karşısında gerçeklemesi esnasındaki performansı incelendiğinde Şekil 4.5'de sunulduğu gibi imza doğrulama isteği sayısı 1000 ve üzerine ulaştığında, ortalama cevaplanma süresi 1 dk'nın üzerine çıkabildiği görülmüştür.

Performans çözümleri için, önerilen çok katmanlı YM modeli ile gelen istekler farklı YM'ye dağıtılarak performansın arzu edilen seviyelere çekilmesi mümkündür. Modelde, gizli ve açık imza anahtar ikilisini üreten birim ile YM'nin aynı birim olması zorunluluğu yoktur. Çünkü yetki bilgisi ile hazırlanan yetkili imza anahtarı ile üretilen imza, var olan açık anahtar ile doğrulanabilmektedir.



Şekil 4.5: Yetkilendirme makamı yetki bilgisi üretme ve doğrulama performans değerleri

Önerilen çalışma, yetkinin denetimi için yetki bilgisine ihtiyaç duymaktadır. Bu ek verinin taşınması ek bir yük getirse de, bu yapı ile yetki denetimi arşivlenmiş imzalı belgeler ve kurumlar arası yazışmalarda gereksinim duyduğu yetki kanıtına sahip olmaktadır.

4.3. Güvenilirlik ve Sistem Güvenliği Analizi

Çalışmada yapılan erişilebilirlik analizi, iş akışındaki tetikleme ve çakışıklık matrisleri ile hesaplanmış ve doğrulamada Petri ağı performans ve güvenilirlik analizi aracı PIPE [46], [47]'den faydalanılmıştır. Erişilebilirlik analizi, iş akışı ve analiz yapılırken örneklenen tetiklemeler (işaretler) uygulandığında aynı sonuçlar alınacağından, güvenilirdir. Literatürde, yetki denetiminde kimlik denetiminin yetersizlikleri ortaya konulmuş ve çözüm önerileri sunulmuştur [9], [38]. Çıkarım olarak sunulan yetki denetimindeki zafiyetler, bu çalışmalarla çelişmediği ve ilgili çalışmaları analiz ile desteklediği için güvenilirdir.

Tüm kurumsal seviyeler ve YM hiyerarşisi arasındaki iletişimin, güven mekanizmaları veya şifreleme gibi yeterli güvenlik seviyesi sağlanarak yapıldığı varsayılmaktadır. Modelde, gizli ve açık imza anahtar ikilisini üreten birim ile YM'nin aynı birim olma gereksinimi yoktur. Böylelikle YM, kullanıcı u_a'ya ait gizli anahtarı bilmediğinden, yetkibilgisini üreten taraf olmasına rağmen u_a gibi görünerek yetkili imzayı oluşturamaz. Yetkili imza anahtarının doğrudan paylaşılmaması ve üretilirken imzaya özel, tek kullanımlık rastgele sayı kullanılması, aradaki adam saldırısını engellemektedir. Yetki bilgisi, sahip olunan kişiye aitlik ve YM'nin onayını taşıma özelliklerine sahip olduğundan; üçüncü taraf, başkasının yetki bilgisi ve kendi imza anahtarıyla geçerli yetkili imza veya bu amaçla sahte yetki bilgisi üretemez. Yetki bilgisinin doğru kaynakta üretilip üretilmediği taşıdığı onay imzası ile kontrol edilebilirdir. Bu ve benzeri durumlarda YM'nin doğruluğu sorgulanacaksa yetki bilgisindeki açık anahtar kullanılmamalıdır. Sunulan şemanın güvenlik analizi takip eden bölümde sunulmuştur.

4.4. İmza Şemasının Rastsal Kâhin Modeli ile Güvenlik Analizi

Random Oracle (Rastsal Kahin) Modeli [48] pratik uygulamalarda Bellare ve Rogaway tarafından önerilmiş olup analizlerde saldırgan da dâhil tüm tarafların erişebildiği bir kahine (oracle) sahip olduğu varsayılır. Random oracle (RO) genelde bir özetleme fonksiyonunun soyutlanması ile elde edilen ve nasıl çalıştığı bilinmeyen

bir kara kutuyu temsil eder; öyle ki RO yapılan sorguya rastgele bir çıktı üretir ve aynı sorgu için her zaman aynı çıktıyı üretir.

RO, bir kriptografik şemada genel erişime açık olarak inşa edilir ve sorgulara cevap verir. Bir sorgu geldiğinde yaptığı işlem, öncelikle kendi cevap listesinden sorgunun daha önce cevaplayıp cevaplamadığını kontrol etmektir. Eğer listede daha önceden girilmiş herhangi bir kayıt yoksa RO çıktı olarak rastgele bir cevap üretir ve (sorgu, cevap) olarak bunu listesine kaydeder. Eğer sorgu listede yer alıyorsa önceden verilmiş cevabı üretir.

İmzalama benzetiminde, girdi M iletisi üzerinde A yetkibilgisi ile (S, R) imzasında denklem (4.3)'de sunulan eşleme eşitliğinin doğruluğu sorgulanır. Saldırgan, sonunda geçerli imza elde etmeyi umarak benzetim ile seçilmiş ileti saldırısını gerçeklemeye başlar. Saldırı, polinom zamanda gerçeklenmelidir. Saldırgan herhangi bir ileti M, yetki bilgisi A ile $H(M||A)$ ile RO'ya cevabı öğrenmek üzere girdi olarak verir. RO rastgele bir $PR' \in Z_q^*$ ve n' seçip $S' = (n' + r).PR'$'yi hesaplar ve (S', R) ile saldırganı cevaplar. Saldırgan, M üzerindeki imzayı sorgular. İmzalama benzetimi $(S', R) = H(M||A)$ ile RO'yu cevap için sorgular; RO rastgele bir z seçer $S' = z.PR$'yi hesaplar, öyle ki $(S', R) = O(M||A, S')$'dir. Böylece benzetim z ile (S', R)'den oluşan imzayı üretebilecektir. Dikkat edilmesi gereken nokta RO'nun çalışırken farklı yöntemler izlemesidir. Saldırgan imza benzetiminden (S', R)'yi aldığında M iletisi için RO'yu sorgular. RO bu cevabı daha önce ürettiği için cevap listesinden yanıtı çevirir.

Eğer saldırgan, M ile $(S', R) = O(M||A, H(M||A))$ olacak şekilde sahte imza üretebilseydi $e(g, S'), e(PU, R + r.H(A))$ ve rastgele üretilen PR''nin sonucu üretilen PU', rastgele seçilen n' ve z ile üretilen $e(PU', R' + r'H(A))$ eşlemelerinin birlikte polinom zamanda doğrulanabilmesi gerekirdi. Oysa ilk safhada RO ayrık logaritma problemi: $e(g, g^a)$ verildiğinde a'nın bulunması probleminin çözümü, ikinci safhada ise Hesapsal Diffie Hellman problemi: (g, g^a, g^b) den $C = g^{ab}$ elemanının bulunması ile karşı karşıya kalmaktadır. Bu durumda RO'nun polinomsal zamanda sonuç üretmesi varsayımı bu problemlerin polinom zamanda çözümünü gerektirmektedir. Bilinenlere göre ayrık logaritma ve hesapsal Diffie-Hellman problemleri zor kabul edilen hesapsal karmaşıklık sınıflandırmalarındadır. Bu bakımdan, yukarıdaki çözümlerin gerçekleştirilmesi polinom zamanda mümkün

olamayacağından, şema, seçilmiş ileti saldırısıyla sahte imza üretilmesine karşı güvenlidir.

4.5. Erişilebilirlik Analizi

Bir belgenin güvenilirliği, belgenin doğruluğu ve gerçekliğine, içinde vaat edilen bilginin tutarlılığına ve kurumsal ve kurumlar arası boyutta geçerliliğine bağlıdır. Güvenilir bir doküman, kurumsal iş akışında doğru süreçlerden geçerek iş akışına ve kurumsal kurallara uygun olarak üretilmiş olmalıdır. Bu kurallar, yetkilerden yönerge ve politikalara kadar uzanır.

Bu bölümde, her bir katmanda üretilen belgelerin güvenilirliği yetki mekanizmasının etkinliği üzerinden çözümlenmeye çalışılmıştır. Sunulan durumlarda, bir yetki denetimi eğer tüm kullanıcılar için etkili ise etkin olarak kabul edilmektedir. Olası bir zafiyetin ortaya çıkması yetki denetiminin etkin olmadığını gösterecektir.

Peri ağları, literatürde daha önce güvenlik protokollerinin analizinde kullanılmıştır [33], [34]. Bu tezde, iş akışındaki yetki denetimi Petri ağları ile modellenerek; güvenilirlik bu modeller üzerinde incelenmiştir. Erişilebilirlik analizi ile yetki denetimlerinin etkinliği ve iş akışında oluşturulan veya işlem gören belgelerin güvenilirliği sorgulanmıştır.

Karşılaştırmalı bir analiz için $u_a, u_m,\ u_o \in U$ olsun öyle ki u_a yetkili kullanıcı, u_m kötü niyetli kullanıcı ve u_o sistemde tanımlı olmayan saldırgandır. Analizde kullanıcı çeşitliliği açısından saldırgan u_o'nun sistem kullanıcılarına ait bir kimlik bilgisi veya parola gibi bir veriye sahip olmadığı varsayılmıştır. Bir diğer deyişle saldırgan ve kötü niyetli kullanıcı farklılaştırılmıştır.

Bir kullanıcının erişilebilirliği, eğer saldırgan veya kötü niyetli kullanıcı, Petri ağında bir yere erişebiliyorsa kullanıcının iş akışında yetkisiz belge oluşturması veya yetkisiz olarak bir işlem gerçekleştirmesi mümkün olur şeklinde tanımlanmaktadır.

4.6. Çok Katmanlı Yetki Denetim Modelinin İlk Katmanı İçin Erişilebilirlik Analizi

- Oturum Açma Durumu

Saldırgan u_o'nun erişilebilirliği: kimlik doğrulama aşamasını geçemediği için saldırgan u_o, sadece $[t_0\, t_1\, t_2\,]$'yi tetikleyebilir. Durum $[11100]$ ve başlangıç işareti

$[1000000]$'dır. Çakışıklık matrisi $M = M_0 + \mu I$ formülünden $[000100] = [1000000] + [11100] \cdot I$'dır. Saldırgan u_o yer p_3 'e ulaşır ama reddedilir. İş akışı $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_2} M_3$ sırasından sonra u_o için sonlanmıştır.

- Kerberos Durumu

Saldırgan u_o'nun erişilebilirliği: erişim için iki farklı meydan okumayla karşı karşıyadır. İlki normal iş akışında $[t_0\, t_1\, t_2\,]$ geçişleri ikincisi ise doğrudan sunucya erişim denemesidir ki bu da $[t_6\, t_7\,]$ geçişlerinden oluşur. Çakışıklık matrisi $[00010000100] = [1000001000] + [1110001100] \cdot I$ olarak bulunur. Saldırgan u_o ağda sadece p_3 ve p_8 yerlerine ulaşabilir ve $[1110001100]$ tetiklemeleri sonucunda reddedilir. Süreç $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_2} M_3$ veya $M_5 \xrightarrow{t_5} M_6 \xrightarrow{t_6} M_7 \xrightarrow{t_8} M_8$ sıraları ile u_o için sonlandırılır.

Yapılan Petri ağı analizi ilk katmandaki yetki denetiminin saldırgan u_o için etkili olduğunu göstermektedir. Buna rağmen sistem ve iş akışı kötü niyetli kullanıcı u_m için zaafiyet göstermektedir. Kötü niyetli kullanıcı u_m, kimlik doğrulamadan geçebildiği için iş akışında herhangi bir işlemi gerçekleştirebilir. Yetki denetimi için sadece ilk katmanın gerçeklendiği iş akışları kötü niyetli saldırganlar için yetkisiz işleme açıktır.

4.7. Çok Katmanlı Yetki Denetim Modelinin İkinci Katmanı İçin Erişilebilirlik Analizi

İkinci katmanda $[t_0\,]$ tetiklenmediğinden saldırgan u_o kimliğini doğrulayamaz ve başlangıç işareti hiçbir zaman $[1000]$ olamayacaktır. İncelenen durum bu sebepten kötü niyetli kullanıcı u_m'nın Petri ağındaki erişebilirliği üzerinden yapılmıştır.

- Erişim Listesi Durumu

Bu mekanizma, listede kaydı olan ve u_m nin yetkilendirildiği işlemleri gerçeklemesini sağlar. Yetkilendirme doğru çalışıyor gibi görünse de örnek durum yetki denetimi açısından bunun aksini ortaya koymaktadır.

o_{imza} bir belge üzerine imzalama işlemi ve o_{onay} da bir belgeyi, sayısal imza ile onaylama işlemi olarak tanımlansın. Kurumsal iş akışında $u_a$ve u_m , o_{imza} işlemini

gerçeklemeye yetkili olarak bir belgeyi imzalayabilir olsun. Bununla birlikte u_m satın alma biriminde bir personel, u_a ise bu birmin başı olarak tanımlansın ($u_a, u_m \in kullanıcılar, u_a \in şefler$ ve $u_m \in personel$). Sadece u_a'nın bir d satın alma belgesini onay yetkisi olacağı durumda u_a o_{onay} işlemini gerçekleyebilir. Bu durumda, erişim listesi şu kayıt veya kuralları içerir: $\langle kullanıcılar, o_{imza}, izinver\rangle$, $\langle şefler, o_{onay}, izinver\rangle$,$\langle personel, o_{onay}, reddet\rangle$.

Kötü niyetli kullanıcı u_m'nin, $\{u_m, o_{onay}\}$ işlemini gerçekleştirmeyi denediği durumda denetim mekanizması u_m'yi listedeki $\langle personel, o_{onay}, reddet\rangle \wedge u_m \in personel$ kaydı ile sorgulayacaktır. Çakışıklık matrisinden elde edilecek tetikleyiciler $[001000] = [100000] + [11000].I$ olacaktır. Buna göre, $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} M_2 \xrightarrow{t_3} M_3$ sırasını izleyen kullanıcı işlemi gerçekleştiremeyecektir. İş akışı, kötü niyetli kullanıcı u_m için p_3 'de sonlanacaktır.

Bir belgenin onaylanması, iş akışında teknik olarak dokümanın onaylamaya yetkili kişi tarafından sayısal imzalanmasıdır. Satın alma dokümanı d yetkili kişi u_a tarafından imzalanarak onaylanabilir. İş akışında, kötü niyetli kullanıcı u_m, $o_{approve}$ işlemini listedeki kurallardan dolayı gerçekleştiremez ama yine listenin zayıf yanından faydalanarak P2'de yetki denetimini atlatabilir. $\langle personel, o_{imza}, izinver\rangle \wedge u_m \in personel$ kaydı ile d üzerinde o_{imza} işlemini P5'de gerçekleyebilir. Yetki ve işlem tanımlamalarındaki eksiklik iş akışındaki yetki denetimini etkisizleştirmektedir. Mekanizma, bir belgeyi yetki kontrolüne uğramadan onaylanmış gibi imzalamaya açıktır. Erişim listesindeki kayıtların kurumsal işlemlerin tanımlanması için kısıtlı olduğu ve listelerin tüm işlem tanımları ve iş akışındaki, yükselme, iptal, devretme gibi yetki dinamizmine uyumunun ise yönetim zorlukları getirdiği önceki bölümlerde ifade edilmiştir[9]. Üçüncü katman, listelerin bu problemlerini adreslemek üzere devreye girmektedir.

4.8. Çok Katmanlı Yetki Denetim Modelinin Üçüncü Katmanı İçin Erişilebilirlik Analizi

Üçüncü katmanda da $[t_0]$ tetiklenmediğinden saldırgan u_o kimliğini doğrulayamaz ve başlangıç işareti hiçbir zaman [1000000] olamayacaktır. İncelenen durum bu sebepten kötü niyetli kullanıcı u_m'nın Petri ağındaki erişebilirliği üzerinden yapılmıştır.

• RBAC Durumu

Bu mekanizma ile kötü niyetli kullanıcı u_m'nin sadece rolü çerçevesinde işlem gerçekleştirebileceği sağlanmaktadır. Rol tabanlı yaklaşım, kurumsal süreç ve işlemleri kurumsal roller ve kullanıcı izinleri ile çözümlemektedir.

Kötü niyetli kullanıcı u_m, $\langle personel, o_{onay}, reddet\rangle \wedge u_m$ "$personel$" rolüne $sahiptir$ kuralı ile $\{u_m, o_{onay}\}$ işlemini gerçekleştirmek istediğinde erişilebilirliği $\{P0, P1, P5, P4\}$ yerlerinden geçişlerle oluşan $M_0 \xrightarrow{t_0} M_2 \xrightarrow{t_5} M_3 \xrightarrow{t_6} M_4$ sırası olacaktır ve u_m işlemi gerçekleştiremeyecek ve iş akışı yer $P4$.'de sonlanacaktır.

Yetkili kullanıcı u_a ise yer $P7$'de $\{u_a, o_{onay}\}$ işlemini $\langle şefler, o_{onay}, izinver\rangle \wedge u_a$ "$satın\ alma\ birim\ şefi$" rolüne $sahiptir$ yetkisini kullanarak gerçekleştirebilecektir.

İşlemler rollerde detaylı olarak tanımlanabildiğinde yetkisiz işlem gerçekleştirilmesi önlenmiş olmaktadır. RBAC, SoD kuralına göre göre sistemdeki bir kullanıcı eğer satın alma emrini hazırladıysa aynı zamanda kendisi onaylayamaz. SoD r rolünü $r : o_{onay} \rightarrow u \wedge \nexists r: o_{onay} \rightarrow u$ kuralına uymaya zorlar.

4.9. Çok Katmanlı Yetki Denetim Modelinin En Üst Katmanı İçin Erişilebilirlik Analizi

Bu katmanda gerçeklenen mekanizma yardımıyla kötü niyetli kullanıcı u_m kurum yönergeleri göz önünde bulundurularak rolünün izin verdiği işlemleri yetkisi doğrultusunda gerçekleştirebilmesi için yönlendirir.

• Yönerge Durumu

Erişilebilirlik analizine göre, kötü niyetli kullanıcı u_m, $\langle o_{onay}, e_{satınalmaonayı}, personel, u_m, d_i\rangle \wedge u_m$, "$personel$"rolüne $sahiptir \wedge$ d_i $personel$ rolü için $o_{onay} \rightarrow \{0\}$ kurallarının varlığında $\{u_m, o_{onay}\}$ işlemini gerçekleştirmeyi dener. $M_0 \xrightarrow{t_0} M_2 \xrightarrow{t_5} M_3 \xrightarrow{t_6} M_4$ sırası tetiklenerek, kötü niyetli kullanıcır u_m işlemi gerçekleştiremez ve iş akışı yer $P4$'de sonlanır.

Eğer kötü niyetli kullanıcı u_m, iş akışında imza işlemi ile oluşturduğu bir belgeyi onaylı belge olarak sunmak isterse süreçte, işlem için sağlanan yetki bilgisi yardımıyla bu yetkisiz işlem tespit edilir. Kötü niyetli kullanıcı u_m, $\langle o_{imza}, e_{kişiselimza}, personel, u_m, d_i\rangle \wedge u_m$ "$personel$" rolüne sahiptir $\wedge$ d_i $personel$ rolü için $o_{imza} \rightarrow \{1\}$ kurallarının varlığında $\{u_m, o_{imza}, e_{kişiselimza}\}$ işlemini $P7$'de gerçekleştirir. İşlem türü, imzalı belgenin onay olarak sürece dahil edilmesini önler. İşlem $\{u_m, o_{imza}, e_{kişiselimza}\}$ olarak tanımlanır.

Üçüncü katmandaki yetki denetiminin aksine, kullanıcının süreci atlatarak güvenilirliği zayıflatması mümkün olmamaktadır. Bununla beraber, dördüncü yetki denetim katmanı, kurumsal yönergelerin bilgiler ile aktarılması ile yetkisiz işlem tespitini sağlamaktadır. Üçüncü katmanda yer alan yetki vekaleti, yönergeler dahil edilerek bu katmanda daha hassas bir seviyeye çıkarılır.

Kullanıcı u_m, $\langle o_{onay}, e_{onayvekaleti}, personel, u_m, d_i\rangle \wedge u_m$ "$onay\ vekaleti$" rolüne sahiptir $\wedge$ d_i *" vekil onay makamları en fazla ... TL miktarına kadar onay izni vardır"* $o_{onay} \rightarrow \{1\}$ yönerge ve kurallarının varlığında yetki vekaleti ile $\{u_m, o_{onay}, e_{onayvekaleti}\}$ işlemini gerçekleştirebilir. İşlem yönergede belirtilen d_i kuralının r_d rolüne uygulanmasıyla kısıtlanmıştır. İşlem tipi onay olarak tanımlanmaktadır. Kötü niyetli kullanıcı u_m kurumsal yönergelerin dışında yetkisiz bir işlemi gerçekleştiremez veya yetkisiz bir işlemi yetki denetiminden geçiremez.

Her bir katman yetki anlamında güvenilirliğe katkıda bulunmaktadır. Ama bu katkılar tek başlarına yeterli olmamaktadır. Her katmanda, yetki denetim seviyesi artmaktadır. Her katmanda yetki tanımına eklenen bilgiler, güvenilirliğin doğrulanması sürecinde yetki denetimini destekler.

4.10. Modelin Genel Analizi

Yetki denetimindeki hassasiyetin ölçüsü yetki ile ilişkilendirilen bilgidir. İlk katmanda, bu, kullanıcının kimlik bilgisi biçimindedir. Üst katmanlara çıktıkça bu bilgi artarak, listede tanımlı işlemler, roller, süreçler ve kurumsal yönerge ve politikalar ile donatılmaktadır. Yetki a ve onay y tanımları her katmanda yetki denetiminin hassasiyetine katkıda bulunmaktadır.

Yetki denetimindeki karmaşıklık yetkinin kapsamı ile ilişkilidir. İlk katmanda, yetki kontrolü kullanıcı kimliği ile sistem erişimi izni sağlar. En üst katmanda yetki denetimi için kurumsal yönergeler dikkate alınmalıdır. Her bir katmanda yukarı çıkıldıkça yetkinin doğrulanması ve bu bilginin yönetimi bir öncekine göre daha karmaşıklaşmaktadır.

Yetki denetimi süreci sonunda elde edilen doğrulanmış işlem kümesi modelin katmanlarının bir diğer özelliğidir. Yetki denetiminin işlemler bakımından kapsamı bu küme ile tanımlanmaktadır. Her katmanda, yetki a içerisinde tanımlanan $o \in O$ bu kapsamı belirtir. İlk katmanda, yetki denetimi genel sistem erişim yetkisi sağlar ki bu en geniş işlem kümesidir. Daha üst katmanlara çıkıldıkça işlemler özelleşmekte ve kapsam daralmaktadır.

İşlemsel kapsamın yanında yetki denetiminin bir de kullanıcı kapsamı yönü vardır. İşlemsel kapsam ile benzer özellik gösteren ve kullanıcılar kümesinin genelden daha da özele daraldığı bu tanımlama da yetki denetiminin uygulandığı veya geçerli olduğu kitleyi belirler. İlk katmanda yetki denetimi tüm $u \in U$ kullanıcıları kapsar. Daha sonra yetki denetimi roller, gruplar ve işlemlere göre özelleşir.

5. SONUÇLAR ve YORUMLAR

Bu bölümde tez çalışmasının sonuçları ve yapılan analizler yar almaktadır.

5.1. Özgün Katkılar ve Tartışmalar

Kerberosun dağıtık sistemlerde yetkilendirme konusundaki eksiklikleri ve güvenlik için yetkilendirme mekanizmasına ihtiyaç duyduğu bilinmektedir. Çalışmada yapılan erişilebilirlik analizi sadece kimlik denetimi yapılmasının iç saldırganın yetkisiz belge üretebilmesinin önüne geçemediğini ortaya koymakta ve desteklemektedir. Erişim denetim listeleri, kullanıcı ve işlemler için sahip oldukları kısıtlı tanım aralıklarından dolayı, iş akışında karmaşıklaşan işlemler söz konusu olduğunda yetersiz hale gelmektedir. Bilindiği gibi rol tabanlı erişim denetimi yöntemleri, erişim denetim listelerinin yetersizliklerine çözüm olarak önerilmiştir. Kullanıcıların, genel tanımlarla yapılmış yetki kısıtlamalarını, iş akışında atlatarak yetkisiz belge üretimi/onayı yapabildiği erişilebilirlik analizi ile sunulmuştur.

Sayısal imzalar tasarlanırken belgenin özgünlüğünün korunması ve kimlik doğrulama fonksiyonları ön planda tutulmuş ama kurumsal iş akışındaki politika ve yönergeler imzaya ait iç parametreler olarak imza şemalarında şimdiye kadar yer bulamamıştır. Örnekleri sunulan farklı imza şemalarında, kişisel imza yetkilendirmelerinin düzenlenmesi söz konusuyken kurumsal yetkinin kullanımı ve kurumsal yetkilerin imza ile denetlenebilmesini hedeflenmemektedir. Söz konusu çalışmalarda imza ile ilişkilendirilen bilgi, çalışmayla sunulan şemada imzaya eklenen kurumsal imza yetkilerini içermemektedir. Belirtilen eksikliklere çözüm getiren çalışma bu bakımdan özgün niteliktedir.

5.2. Sonuç ve Öneriler

Bu çalışmada, kurumsal iş akışındaki belgelerde, yetki denetiminin, kurumlar arası ve arşiv gibi süreç dışındaki sürdürülebilirlik problemi sunulmuş ve problemin Petri ağları yöntemi ile yapılan analizinde kurumsal iş akışında yetki denetiminin eksiklikleri değerlendirilmiştir. Vaka çalışması olarak kurumsal uygulamalarda, yetki

politikalarına ve imza yetkisi yönergelerine tabi olan onay belgeleri üzerinde yetki denetimi ele alınmıştır. Önerilen model gerçeklenerek, güvenlik ve performans analizleri yapılmış ve pratikte kullanılabilirliği tartışılmıştır. Yetkilendirme makamı için farklı mimariler önerilerek modelin uyumluluğu ve geliştirilebilirliği artırılmıştır.

5.3. Kullanım Alanları

Çok katmanlı yetki denetim modeli, temel olarak yetki denetim yöntemlerini, yetki denetim sürecine katkıları, birbirleriyle ilişkilerini ve yöntemlerin analizini yapmak amacıyla önerilmiştir. Daha önce yetki denetim yöntemlerinde ele alınmayan kurumsal yönergelerden kaynaklanan problemlere çözüm olarak önerilen bir yetki denetim yöntemi sunulmuş ve modelde dördüncü ve üst seviyeye yerleştirilmiştir.

Model, kurumsal iş akışında yetki denetim uygulayıcıları için temel bir rehber niteliğindedir. Uygulayıcılar, katmanların yeteneklerini göz önünde bulundurarak gereksinimlerine göre sistemlerinde mekanizmaları yapılandırabilirler. Karar vericiler, modeldeki katmanların kapsam ve işlevsel sınırlarına göre gerekli gördükleri yetki denetim mekanizmalarına karar verebilirler.

Model, uygulayıcıların kendi sistemlerini analiz edebilecekleri sistem iş akışı için bir şablon sunmaktadır. Analiz sonucunda gereksinimlerini karşılamadığı düşünülen uygulamalar için, sistemlerinde bir üst katmanda yer alan yetki denetim mekanizmasını gerçekleyerek iyileştirme yoluna gidebilirler.

Önerilen model tek kullanıcılı, kullanıcının tüm yetkiye sahip olduğu sistemler için kullanışlı değildir. Bu ve benzeri sistemler kullanıcıya ya tüm erişim haklarının verildiği ya da tüm erişimlerin reddedildiği tek bir katmandan oluşurlar. Mobil istemciler veya dağıtık sistemler için model ilk analiz adımı için kullanılarak yetki denetim gereksinimi veya ihtiyaç duyulan mekanizmanın çıkarılması için kullanılabilir.

Model, yetki denetiminin yüksek önem arz ettiği kurumsal iş akışlarını temel almaktadır. Çoğu sistemde, yönetmeliklerde tanımlanan kurumsal yetkiler, yetki denetiminde karşılık bulmamaktadır. Model ile önerilen üst katman ile bu yetki denetim zafiyetini ortaya konularak bir çözüm önerisi sunulmaktadır.

Model, yetki denetim yapılandırmasının nihai halini aldığını öne sürmediği halde özel yetki denetim gereksinimlerine ihtiyaç duyan uygulamalar için modelin

üstünde başka bir katmanın konulmasını önlemeyecek şekilde yapılandırılmıştır. Çok katmanlı model, var olan çok yetkili sistemlerdeki yetki denetim mekanizmalarının incelenmesi için bir rehber olabilir. Bu gözden geçirme yetki denetim kapsamının güncellenmesi ve var olan katmandan bir üst katmana geçişi tetikleyebilir. Önerilen model, var olan sistemin analizi ve fark edilmeyen kritik zafiyetlerin ortaya çıkarılması için kullanılabilecek yetenektedir.

Katmanlardaki yetki denetim mekanizmalarının kurumsal yönerge eksiklikleri sunularak, kurumsal yönerge içeren bir yetki denetim yöntemi önerilmiştir. Önerilen model ile iş akışındaki bir belgenin yetkisi erişilebilirlik analizi ile yapılabilecektir. Eğer belge üzerinde yetkisiz bir işlem yapılmışsa yöntem bunu açığa çıkaracak şekilde planlanmıştır.

Bununla beraber, çok katmanlı yetki denetim modelinin son katmanı için önerilen yönerge temelli yöntem, iş akışındaki bir belgenin güvenilirliğini destekleyecek niteliktedir. Yöntem, bilinen yetki denetim mekanizmalarının eksik kaldığı kurumsal politika ve yönergelere uyumlu olarak yetki denetimini sağlamaktadır.

Bu tezde, bir, çok katmanlı yetki denetim modeli önerilmiştir. Model, yetki denetim mekanizmalarının işlevsellikleri, yetki kapsam ve hassasiyetleri, işlemsel kapsam ve yetki denetim etkinlikleri üzerine kurulmuştur. Katmanların, bir iş akışında belge güvenilirliğine yaptığı katkılar, Petri ağları üzerinde erişilebilirlik analizi ile incelenmiştir.

Petri ağları ve analizler, iş akışına mekanizmaların işleyişini göz önüne koyarken yöntemlerin yetki denetim eksikliklerine de ışık tutacak şekilde basit tutulmuştur. Erişilebilirlik analizinin yetki denetim için kullanılması daha gelişmiş iş akışı modellerinde farklı problemlerin açığa çıkarılması için yararlı olabilir.

Petri ağları genellikle iş akışındaki aksaklıkların çıkarılması için kullanılmıştır. Bilindiği kadarıyla, bu çalışma ile erişilebilirlik analizi ilk defa iş akışlarında yetki denetimi için kullanılmaktadır.

Önerilen model ve yetki denetimi üzerindeki erişilebilirlik analizi iş akışlarında süreğen yeniden yetkilendirme için kullanışlı bir araç olacaktır. Yönerge temelli yetki denetimi, iş akışındaki yetkisiz işlemlerin tespiti için basit ve etkin bir çözümdür.

Bu çözüm, aynı zamanda güvenilirlik için doğrulamada kullanılacak yetki verisi sağlamaktadır. Önerilen çözümün yönetim maliyeti, kurumsal politika ve yönergelerin işlevsel olarak yetkiye dâhil edilmesinden kaynaklanan bir fazlalığa sahiptir.

Bu çalışmada, sadelik açısından, farklı özellikteki en temel yöntemler modele dâhil edilmiştir. Çok katmanlı yetki denetim modeline yetki denetim yetenekleri farklı yöntemler eklenerek model katmanları geliştirilebilir. Katmanlar bir bütün olarak ele alınmasına rağmen birden fazla mekanizma bir katmanı bölebilir veya paylaşabilir.

KAYNAKLAR

[1] Web 1, (2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/ 2014-us-state-of-cybercrime.html, (Erişim Tarihi: 14/11/2014).

[2] Web 2, (2013), http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58738 , (Erişim Tarihi: 29/09/2014).

[3] Schneier B., Ranum M., (2009), "Schneier-Ranum. Face-Off: Is Perfect Access Control Possible?", Information Security Magazine, 11 (8), 13-15.

[4] Poovendran R., Narayanan, S., (2005), "Protecting Patient Privacy Against Unauthorized Release of Medical Images in A Group Communication Situation", Computerized Medical Imaging and Graphics, 29, 367-383.

[5] Fakhari P., Vahedi E., Lucas C., (2011), "Protecting Patient Privacy From Unauthorized Release Of Medical Images Using A Bio-Inspired Wavelet-Based Watermarking Approach", Digital Signal Processing, 21, 433-446.

[6] Neuman B. C., Ts'o T., (1994), "Kerberos: An Authentication Service for Computer Networks", IEEE Communications, 32, 33-38.

[7] Rigney C., Rubens A., Simpson W., Willens S., (1997), "Remote Authentication Dial In User Service (RADIUS)", RFC, 2138, 1-64.

[8] Jie W., Arshad J., Sinnott R., Townend P., Lei Z., (2011), "A Review of Grid Authentication and Authorization Technologies and Support for Federated Access Control", ACM Computing Surveys, 43 (2), 1-26.

[9] Barkley J., (1997), "Comparing Simple Role Based Access Control Models and Access Control Lists", Proceedings of RBAC '97, 127-132, NY, USA, 6-7 Nov.

[10] Ferraiolo D. F., Kuhn R., Sandhu R., (2007), "RBAC Standard Rationale: Comments on a Critique of the ANSI Standard on Role Based Access Control", IEEE Security & Privacy, 5, 51-53.

[11] Locke G., (2009), "Digital Signature Standard (DSS)", FIPS, 186 (3), 1-119.

[12] Tan K., Crampton J., Gunter C., (2004), "The Consistency of Task-Based Authorization Constraints in Workflow", In Proceedings of The 17th IEEE Computer Security Foundations Workshop, 155-169, NY, USA, 28-30 June.

[13] Dempsey K., Ross R. S., Mcguire K. S., (2014), "National Institute of Standards and Technology (NIST) Supplemental Guidance on Ongoing Authorization (OA)", NIST, 800 (37), 1-10.

[14] Web 3, (2016), http://www.interpares.org/, (Erişim Tarihi: 05/02/2016)

[15] Külcü Ö., (2012), "Türkiye'de Kurumsal Elektronik Bilgi ve Belge Yönetimi Uygulamalarına Dönük Koşulların Değerlendirilmesi: 57 Örnek Kurumun Analizi", Türk Kütüphaneciliği, 26 (1), 7-30.

[16] Umut G., Külcü Ö., (2014), "Elektronik Belge Yönetimi Uygulamalarında Karşılaşılan Sorunların Analizi ve Çözüm Önerileri: Kalkınma Bakanlığı Örneği", Bilgi Dünyası, 15 (1), 102-124.

[17] Mambo M., Usuda K., Okamoto E., (1996), "Proxy signatures: Delegation of The Power To Sign Messages", IEICE Trans. Fundamentals, E79-A (9), 1338-1354.

[18] Chaum D., Heyst E. V., (1991), "Group Signatures", LNCS, 547, 257–265.

[19] Bellare M., Shi H., Zhang C., (2005), "Foundations of Group Signatures: The Case of Dynamic Groups, Topics in Cryptology", LNCS, 3376, 136–153.

[20] Shamir A., (1984), "Id- Based Cryptosystems and Signature Schemes", LNCS, 196, 47-53.

[21] Paterson K. G., (2002), "ID-Based Signatures From Pairings On Elliptic Curves", IEEE Communication Letters, 38 (18), 1025-1026.

[22] Yortanli A., (2011), A Certificate Based, Context Aware Access Control Model For Multi Domain Environments, Master Thesis, Middle East Technical University.

[23] Kuhn R., (2004), "American National Standard for Information Technology—Role Based Access Control", BSR INCITS, 359, 1-49.

[24] Elektronik İmza Kanunu, (2004), Kanun No:5070, Sayı: 25355, 3 Ocak 2004 Tarihli Resmi Gazete.

[25] Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliskin Tebliğde Değisiklik Yapılmasına Dair Tebliğ, (2006), Sayı: 26056, 21 Ocak 2006 Tarihli Resmi Gazete.

[26] Diffie W., Hellman M. E., (1976), "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6), 644-654.

[27] Rivest R., Shamir A., Adleman L., (1978), "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communication of ACM, 21 (2), 120-126.

[28] Yılmaz B., (2008), "Applications of Petri Nets", Master Thesis, Izmir Institute of Technology.

[29] Başkocagil C., (2014), "Demiryolu Anklaşman Sistemlerinin Petri Ağları ile Tasarımı ve Gerçeklenmesi", Doktora Tezi, İstanbul Teknik Üniversitesi.

[30] Lui R. W. C., Hui L. C. K., Yiu S. M., (2007), "Delegation with Supervision", Information Sciences, 177 (19), 4014-4030.

[31] Coyne E., Weil T. R., (2013), "ABAC and RBAC: Scalable, Flexible ,and Auditable Access Management", IT Professional, 15, 14-16.

[32] Hardt D., (2012), "The OAuth 2.0 Authorization Framework", IETF RFC, 6749, 1-76.

[33] Jensen K., (1992), "Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use", 1st Edition, Springer.

[34] Al-Azzoni I., Down D. G., Khedri R., (2005), "Modelling and Verification of Cryptographic Protocols Using Coloured Petri Nets and Design", Nordic Journal of Computing, 12 (3), 72-91.

[35] Zaitsev D. A., (2013), "Clans of Petri Nets: Verification of Protocols and Performance Evaluation of Networks", 1st Edition, LAP LAMBERT Academic Publishing.

[36] Boneh D., Lynn B., Shacham H., (2001), "Short Signatures From Weil Pairing", LNCS, 2248, 297-318.

[37] Web 4, (2004), http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html, (Erişim Tarihi: 14/11/2014).

[38] Yuqing S., Qihua W., Ninghui L., Bertino E., Atallah M., (2011), "On the Complexity of Authorization in RBAC under Qualification and Security Constraints", IEEE Trans. Dependable Secure Computing, 8 (6), 883-897.

[39] Fakhari P., Vahedi E., Lucas C., (2011), "Protecting Patient Privacy From Unauthorized Release of Medical Images Using a Bio-Inspired Wavelet-Based Watermarking Approach", Digital Signal Processing, 21, 433-446.

[40] Adams C., (2008), "PKI, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF RFC, 5280, 1-95.

[41] Farrell S., Housley R., (2002), "An Internet Attribute Certificate Profile for Authorization", IETF RFC, 3281, 1-40.

[42] Cooper D., (2008), "PKI, Internet X.509 Public Key Infrastructure Profile", IETF RFC, 5280, 1-151.

[43] Joux A., (2000), "A One Round Protocol for Tripartite Diffie-Hellman", Proc. of the 4th International Symposium on Algorithmic Number Theory, 1st Edition, Springer-Verlag.

[44] Web 5, (2014), http://crypto.stanford.edu/pbc/, (Erişim Tarihi, 29/09/2014).

[45] Web 6, (2014), http:// gmplib.org, (Erişim Tarihi, 29/09/2014).

[46] Dingle N. J., Knottenbelt W. J., Suto T., (2009), "PIPE2: A Tool for The Performance Evaluation of Generalised Stochastic Petri Nets", ACM SIGMETRICS Performance Evaluation Review, 36 (4), 34-39.

[47] Web 7, (2014), http://pipe2.sourceforge.net/, (Erişim Tarihi, 14/11/2014).

[48] Bellare M., Rogaway P., (1993), "Random Oracles are practical: A Paradigm for Designing Efficient Protocols", ACM Conf. Computer and Communication Security, 1993, 62-73.

ÖZGEÇMİŞ

Alper UĞUR 1978 yılında Sivas'ta doğdu. 2001 yılında Yeditepe Üniversitesi Mühendislik ve Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Daha sonra Araştırma görevlisi olarak başladığı Pamukkale Üniversitesi'nde kriptografik güvenli haberleşme konusunda yüksek lisans yaptı. Bir süre Gebze Yüksek Teknoloji Enstitüsü Ağ ve Bilgi Güvenliği Laboratuvarı'nda görev yapan Alper UĞUR, Türk Bilişim Derneği'nde Cisco Academy Eğitmeni olarak gönüllü eğitimler vermiştir. 2014 yılından bu yana Pamukkale Üniversitesi'nde bilgi güvenliği ve kriptografi konularında araştırmalarına devam etmektedir.

EKLER

Ek A: Tez Çalışması Kapsamında Yapılan Yayınlar

Uğur A., Soğukpınar İ., (2006), "Elektronik İmza Uygulamalarının Sürekliliği İçin Tasarım Kalıplarının Kullanılması", 1. Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, 35-40.

Uğur A., Soğukpınar İ., (2006), "Yazılım Mimarisinin Evrimi Üzerine bir Durum Çalışması: Elektronik İmza Uygulamasının Sürekliliği", 1.Ulusal Yazılım Mimarileri Konferansı Bildiriler Kitabı, 138-142

Uğur A., Soğukpınar İ., (2007), "A New Hierarchical Signature Scheme with Authorization", Proc. Information Security and Cryptology Conference, 47-50.

Uğur A., Soğukpınar İ., (2009), "A Framework for Licensed Digital Signatures". Proc. NetCoM 2009, 428-432.

Soğukpınar İ., Uğur A., (2010), "H-Yetkim: Hiyerarşik Yetkili İmza Modeli Tasarlanması ve Eşleme Tabanlı Kriptografi İle Akıllı Kartlar Üzerinde Gerçeklenmesi", TUBİTAK Proje, 108E132.

Uğur A., Soğukpınar İ., (2010), "An X.509 Based Licensed Digital Signature Framework for Hierarchical Organizations",Recent Trends in Wireless and Mobile Networks: Second International Conference, Ankara, Turkey, 26-28 June.

Uğur A., Soğukpınar İ., (2014), "Sustainable Authorization in Enterprise Workflow and Authorized Digital Signature Model", Journal of the Faculty of Engineering and Architecture of Gazi University; Cilt 29, Sayı 3, 559-568.

Uğur A., Soğukpınar İ., (2016), "Multi-Layer Authorization Model and Analysis of Authorization Methods", Turkish Journal of Electrical Engineering & Computer Sciences Available online: 03.10.2015 Last modified on 17.05.2016