Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 29, No 3, 559-568, 2014

Journal of the Faculty of Engineering and Architecture of Gazi University
Vol 29, No 3, 559-568, 2014

KURUMSAL İŞ AKIŞINDA SÜRDÜRÜLEBİLİR YETKİ DENETİMİ VE YETKİLİ SAYISAL İMZA MODELİ

Alper UĞUR[1], İbrahim SOĞUKPINAR[2]
[1,2]Gebze Yüksek Teknoloji Enstitüsü, Bilgisayar Mühendisliği Bölümü
[1]augur@bilmuh.gyte.edu.tr,[2]ispinar@bilmuh.gyte.edu.tr

(Geliş/Received: 24.12.2013; Kabul/Accepted: 01.07.2014)

ÖZET

Yetki denetim sistemleri, kurumdaki kullanıcının, ait olduğu fonksiyonel gruba tanımlanan izinler doğrultusunda işlem yapabilmesine olanak tanımaktadır. Kurum içi iş akışında uygulanan bu denetim, yetki kontrolünde kurumlar arası yazışmalar gibi kurum yapısı dışına çıkan süreçlerde yetersiz kalmaktadır. Bu çalışmada, yetki denetiminin, kurumsal iş akışında, dolaşımda ve arşivlenen belgeler kapsamında süreklilik analizi, petri ağları yöntemi ile ortaya konulmuştur. Kurumsal yetki denetimindeki eksiklikler için sayısal imza üzerinde bir vaka çalışması yapılmış ve yetki denetiminin sürdürülebilirliği için imzanın yetki denetimi işleviyle donatıldığı bir çözüm modeli önerilmiştir. Bu çözüm, eşleme tabanlı kriptografi ile gerçeklenmiş ve yapılan analizler çalışmaya dâhil edilmiştir.

Anahtar kelimeler: Sayısal imza, Yetkilendirme, Kurumsal yetkiler

SUSTAINABLE AUTHORIZATION IN ENTERPRISE WORKFLOW AND AUTHORIZED DIGITAL SIGNATURE MODEL

ABSTRACT

Authorization systems makes it possible that a user could only act in accordance with the permissions defined by the functional group it belongs. The authorization control mechanism employed in workflow became insufficient for the external enterprise processes as inter-agency correspondences. In this study, the sustainability of authorization in enterprise workflow, documents in circulation and long-term archives has been analyzed and demonstrated with Petri net models. Furthermore, a case study on digital signatures for the deficiencies of the enterprise authorization is presented. An authorized signature model is also proposed where authorization is employed in digital signature for the sustainability of authorization. The proposed solution is implemented using pairing based cryptography and analyses are provided.

Keywords: Digital signature, Authorization control, Enterprise authorization

1. GİRİŞ (INTRODUCTION)

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. Belge üzerinde yetki dahilinde yapılan bu işlemler belgeyi geçerli kılar.

Uygulamalarda, sistem giriş yetkisinden erişim denetimine kadar, bir çok gelişmiş yetkilendirme mekanizması kullanılmaktadır. Bu mekanizmalar, iş akışında, varlıkların sürece dahil 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.

Anlık kurumsal iş akışında dolaşımdaki belgelerde

kişinin işlemin gerektirdiği yetkiye sahip olduğu bilinebilmektedir. Kurumlar arası yazışmalarda ise bu yetki bilgisi, sistemin dışında bir ispat gereksinimine ihtiyaç duymaktadır. Örneğin, A ve B kurumları arasındaki bir yazışmada A kurumundaki a kullanıcısına ait alım işlemi onayı, B tarafı için geçerlilik ifadesi taşımayabilir. Çünkü, A kurumunda iş akışında yetki kontrolü yapılır ifadesi, a kullanıcısının yetkisine dair bir delil değildir. B tarafı, belgeden, a kullanıcısının yaptığı işlem kapsamında A'yı bağlayan geçerli bir kurumsal yetki verisi elde edememektedir.

Süreç dışında yetki denetiminin sürdürülebilirliğine ait bir diğer problem ise arşivlenen belgelerde karşımıza çıkmaktadır. Arşivdeki onaylı bir belgenin, yetki denetiminden geçip geçmediğinin tespitinin doğrudan bir yolu yoktur. Arşive belge yerleştirme ayrıcalığına sahip herhangi bir kullanıcı veya arşiv sistem yöneticisi, onayladığı bir işlem belgesini süreç dışında oluşturup arşive dahil edebilir. Belgeler arşivlenirken yapılan yetki kontrolü ise arşivlenmiş belgelerin yetki geçerliliği sorgusunda doğrudan bir delil sunamamaktadır.

Bu çalışmada, kurumsal işakışındaki belgelerde, yetki denetiminin, kurumlar arası yazışmalar ve arşiv gibi süreç dışındaki sürdürülebilirlik probleminin Petri ağları yöntemi ile analizi yapılmıştır. Ayrıca, kurumsal iş akışında yetki denetiminin eksiklikleri değerlendirilmiştir. Vaka çalışması olarak kurumsal uygulamalarda, yetki politikaları ve imza yönergelerine tabi olan onay belgeleri üzerinde yetki denetimi ele alınmıştır. İmzanın yetkilendirilmesi ile yetki onayının süreç dışında da geçerliliği öngörülmüştür. Bu kapsamda, çözüm için eşleme tabanlı kriptografi kullanan bir yetkili sayısal imza modeli önerilmiştir. Sayısal belgelerin yetkisiz kişilerce imzalanması, önerilen çözüm ile önlenebilinecektir. Önerilen yaklaşım ile kurumsal iş akışında, yetkiler, yazışmalarda yetki denetimi için delil oluşturacak şekilde taşınabilir olmakta ve arşivlenmiş belgelerdeki yetki denetimi problemine bir çözüm sunulmaktadır.

Makalenin organizasyonu şöyledir: Giriş Bölümü'nü takiben Bölüm 2'de ilgili literatür çalışmaları verilmiştir. Bölüm 3'te yetki denetiminin sürdürülebilirliği petri ağları ile analiz edilmiş ve sonuçları sunulmuştur. Bölüm 4'te sayısal imza vaka çalışması üzerinde yetki denetimi problemleri ele alınmış ve çözüm olarak sunulan modelin gerçekleme performansı ve güvenlik analizi verilmiştir. Sonuç ve Öneriler ise Bölüm 5'te sunulmuştur.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

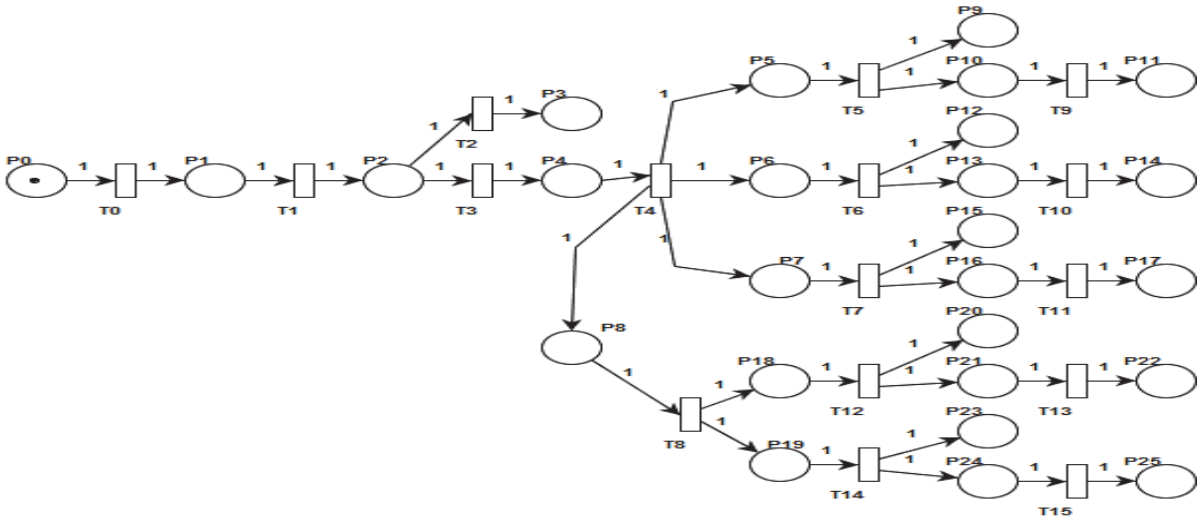
Kurumsal sistemlerde, kullanıcılar, iş akışına dahil olurken karşılarına çıkan ilk yetki kontrolü, sistem erişimini sağlayan kimlik denetimi tabanlı oturum açma mekanizmasıdır. Basit oturum açma, Kerberos[1] ve RADIUS[2] gibi bir çok uygulama kimlik denetimini yetkilendirmede kullanır. Fakat sistem bazında erişim iznini kimlik denetimiyle sağlayan bu tip uygulamalar bazı durumlarda yetkilendirme problemleriyle karşılaşabilmektedir. Erişim denetim listeleri[3], kimlik denetimine ek olarak, kullanıcılar için sistemde tanımlı belirli işlemlere onay veya red girdilerini tutan en temel yetki denetimi uygulamalarındandır. Rol tabanlı erişim denetimi yöntemleri [4], [5] ise kullanıcıları, kurumsal rolleriyle gruplandırarak, işlemlerin bu gruplara tanımlı izinler doğrultusunda gerçeklenmesini destekler.

İmzalı belgelerde yetki konusu, kurumlarda, kurum politikaları, yönetmelik ve yönergelerle belirlenmiştir. Bununla birlikte literatürde imza yetkilendirme üzerine vekil imzalar [6] veya grup imzalar [7], [8] 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 bulunmaktadır. Kendinden sertifikalı ve kimlik tabanlı imza yöntemleri [9], [10] imza anahtarı oluşturulmasına farklı bir açıyla yaklaşan ve imzayı, imzalayana ait bir bilgi ile oluşturma yoluna giden yöntemlerdendir.
Kurumsal bilgi güvenliğinin ve uygulanan güvenlik politika ve protokollerin yeterliliklerinin araştırılması ve testi için birçok yöntem ve uygulama vardır [11]. Literatürde, iş akışlarının modellenmesi ve protokol güvenlik analizinde kullanılan Petri ağları [12], [13], [14] bu çalışmada sürdürülebilirlik ve erişilebilirlik analizinde kullanılmıştır. Örnek vakada üretilen çözüm önerisinde ise eşleme tabanlı kriptografi [15], [16]' den faydalanılmaktadır.

3. YETKİ DENETİM MEKANİZMASININ PETRİ AĞLARI İLE ANALİZİ (PETRI NET ANALYSIS OF AUTHORIZATION MECHANISM)

Bu çalışma ile kurumsal iş akışında yetki denetiminin arşivleme veya kurumlar arası yazışma süreçlerinde yetersiz kalabileceği durumlar ele alınarak yetki denetiminin sürdürülebilirliği problemi Petri ağları üzerinde analiz yapılarak ortaya koyulmuştur. Kurumsal iş akışında üretilen ve imzalanan bir onay/olur belgesinin yetki denetiminden nasıl etkilendiği ve yetki denetiminin yetersiz kaldığı durumlar incelenmiş, yapılan analizde, kurumsal iş akışı petri ağları ile modellenerek, yetki denetiminin sürdürülebilirliği bu model üzerinden gözlemlenmiştir. Model üzerinde uygulanan erişilebilirlik analizi ile iş akışında ortaya çıkabilecek yetkisiz işlemler ve yetkilendirmenin iletimi sunulmuştur.

Bir petri ağı, iş akışındaki durum ve olay kümeleri ile bu iki küme arasındaki ilişkiyi gösteren bir çizgedir. Petri ağı $\sum, \sum = \{\boldsymbol{P}, \boldsymbol{T}, \boldsymbol{F}, \boldsymbol{I}, \boldsymbol{O}, \boldsymbol{M}\}$ beşlisi ile tanımlanır. $\boldsymbol{P} = \{P1, P2, \ldots, PN\}$ sonlu yer kümesi



Şekil 1. Kurumsal iş akışında yetki denetiminin petri ağ modeli (Petri net model of authorization in enterprise workflow)

(durum), $\boldsymbol{T} = \{T1, T2, \dots, TN\}$ sonlu geçiş kümesi (olay) olmak üzere; $\boldsymbol{F} \subseteq (\boldsymbol{PxT}) \cup (\boldsymbol{TXP})$ sonlu yönlü yay kümesi ve $\boldsymbol{I}: (\boldsymbol{TXP}) -> \{0,1\}$ girdi, $\boldsymbol{O}: (\boldsymbol{TXP}) -> \{0,1\}$ çıktı fonksiyonlarıdır. $\boldsymbol{M} = \{M1, M2, .., MI, .., MN\}$, MI, PI yerinde bulunan işaret adedini temsil eder.

Petri ağı üzerinde, $M0$ başlangıç işaretini göstermek üzere, M0'ın varlığında eğer $M0[T1 > M1[T2 > M2 \dots M(K-1)[TK > MK$ şeklinde $T1, T2, \dots TK$ den oluşan bir geçiş dizisi ve $M1, M2, \dots, MK$'den oluşan bir işaret dizisi varsa MK erişilebilirdir.

$U = \{u_1, u_2, \dots u_a, \dots, u_m, \dots u_z\}$ Sistemde tanımlı kullanıcılar kümesi $u_a, u_m \in U$; u_a herhangi bir yetkili kullanıcı, u_m, yetkisiz kullanıcıyı temsil etsin. u_m erişebildiği dokümanlarla sistem akışını, güvenilirliğini bozacak iç saldırgan olsun. 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/ değiştirilmiş, 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 1'de sunulan Petri ağına ait yer ve geçişler Tablo1'de verilmiştir.

Tablo 1. Petri ağı modeline ait yer ve geçişler (Place and transitions in Petri net model)

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

Yetki denetim modelinin ilk aşaması $M0\{P0\}, T0$ başlangıç işaretiyle başlayan ve $M2\{P2\}, T2$ veya $M2\{P2\}, T3$ ile sonuçlanan kimlik denetimini içerir. Bu aşamada sisteme giriş ve sistem kaynaklarını kullanma izni $M0\{P0\}, T0 > M1\{P1\}, T1 > M2\{P2\}, T3 > M3\{P4\}$ 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, çakışıklık 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 $M0\{P0\}, T0 > M1\{P1\}, T1 > M2\{P2\}, T2 > M3\{P3\}$ 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 $M3\{P4\}, T4 > M4\{Px\}$ 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 $M0\{P0\}, T0 > M1\{P1\}, T1 > M2\{P2\}, T3 > M3\{P4\}, T4 > M4\{P5\}, T5 > M5\{P10\}, T9 > M6\{P11\}$ 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 kurumlararası yazışmalarda yetki kanıtı açısından yetersizliğinin incelenmesi üzerinedir. Analiz, takip eden kısımda işakışında bir alım belgesinin onaylanması, arşivlenmesi ve kurumlar arası iletimi örneklenerek yapılmıştır.

Yetkili kullanıcı u_a'nın bir alım belgesini onaylama işlemi iş akışında $T7 > M(k-1)\{P16\}, T11 > Mk\{P17\}$ 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 $T7 > Mk\{P15\}$ ile $P15$'te sonlandırılır.

İç saldırganın yetki denetimini atlatarak d_s'yi oluşturup oluşturamayacağını inceleyelim. Kullanıcı u_m , alım belgesi oluşturma yetkisine sahip olsun, bu durumda $T5 > M(k-1)\{P10\}, T9 > Mk\{P11\}$ 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 $T7^* > M(k-1)\{P16^*\}, T11^* > Mk\{P17^*\}$ 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 $T4 > M(k+1)\{P8\}, T8 > M(k+2)\{P18\}, T12 > M(k+3)\{P21\}$ veya $T4 > M(k+1)\{P8\}, T8 > M(k+2)\{P19\}, T14 > M(k+3)\{P24\}$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, vekalet 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 vekalet etmiş olsun. O zaman zarfında sahip olduğu onay yetkisi, iş akışında $T7 > M(k-1)\{P16\}, T11 > Mk\{P17\}$ 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 dahil 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 $T7 > M(j-1)\{P16\}, T11 > Mj\{P17\}$ sonucunda hazırladığı yetkili d_s ile saldırgan u_m'nin $T5 > M(j-1)\{P10\}, T9 > Mj\{P11\}$ ve $T7^* > M(k-1)\{P16^*\}, T11^* > Mk\{P17^*\}$ 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 2'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 2- 1.a, 5.a), kimlik denetimi ile dış saldırgan engellenmektedir (Tablo2- 1.b, 2-a, 5-b). İşlem yetkilerinin varlığında (Tablo 2- 2.b, 3.b, 4, 6) kullanıcıların yetkileri dahilinde işlem yapmaları sağlanmaktadır.

Arşiv ve kurumlar arası yazışmalar gibi süreçler iş akışında yetki denetiminin kapsamı dışında kalabilmektedir. Bu durum, denetimde zaafiyete 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.

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

4. KURUMSAL İŞ AKIŞINDA YETKİ DENETİMİNİN SÜRDÜRÜLEBİLİRLİĞİ İÇİN BİR VAKA ÇALIŞMASI: YETKİLİ SAYISAL İMZA MODELİ (A CASE STUDY FOR SUSTAINABILITY OF AUTHORİZATION IN ENTERPRISE WORKFLOW: AUTHORIZED DIGITAL SIGNATURE MODEL)

Önerilen Yetkili Sayısal İmza çözümü ile imzaya yetki eklenerek yetkilendirme taşınabilir hale getirilmekte ve bu ek bilgi ile imzalı belgede yetki tespiti gerçekleştirilmektedir.

4.1 Yetkili Sayısal İmza Modeli (Authorized Digital Signature Model)

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

Tablo 2. Yapılan analizin sonuçları (Results of the analysis)

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 ($T5, T6, T7, T12, T14$ tetiklemele rin 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 ($T5, T6, T7, T12, T14$ tetiklemele rin 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	Kullanıcılar ın 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)

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 *yetkibilgisi* 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 2'de X.509 kimlik[17] ve Şekil 3'te öznitelik sertifikalarının[18] *Yetki makamı* (YM), *Yetki Geçerlilik Aralığı* (T-A_i), *Yetki Tanımı* (A_i) ifadeleri ile genişletilmesiyle elde edilen *yetkibilgisi* sertifikası sunulmuştur.

Yetkili sayısal imza, var olan sistemlere uyumluluk göstermesi, kriptografik ve sistem gereksinimlerinden dolayı Açık Anahtar Altyapısı [19] üzerine kurulmuştur. YM'nın modeldeki yeri ve fonksiyonu Şekil 4'te gösterilmiştir. YM temel olarak sertifika yaşam döngüsü görevlerini *yetkibilgisi* kapsamında üstlenir.

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

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

Bu özellikleri taşıyan Tate ve Weil eşlemeleri, anahtar

paylaşımı [20], kimlik tabanlı şifreleme, sayısal imza [15], [16] gibi birçok şemada kullanılmış ve eşleme tabanlı kriptografi kavramını oluşturmuştur.

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 2. Yetkibilgisi X.509 Sertifika Yapısı (Authorization Information X.509 certificate structure)

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

Şekil 4. Yetkibilgisi Öznitelik Sertifika Yapısı (Authorization Information Attribute Certificate Structure)

Önerilen şemanın kayıt, üretim ve doğrulama evreleri: Kayıt sürecinde *yetkibilgisi* YM'da oluşturulur, onaylanır ve imza için kullanılmak üzere imzalayana gönderilir. İmzalayan taraf aynı yetki için YM'na *yetkibilgisi*nin geçerlilik süresi bitmediği sürece tekrar *yetkibilgisi* oluşturmak için başvurmaz ve üretilen *yetkibilgisi* ile yetkili imza anahtarını oluşturur. Yetkili imza anahtarı, (1)'de tanımlanan g üreteç ve PR_i gizli anahtar parametre değerlerinden (2)'de tanımlanan işlemler sonucunda elde edilmektedir.

$$g \in G, e(g,g) \neq 1;\ PR_i \in Z_q^* \quad (1)$$

$$PU_i = PR_i.g \text{ ve } PR_{iA} = PR_i.H1(A) \quad (2)$$

Yetkili sayısal imza, kayıt sürecinde elde edilen yetkili imza anahtarı PR_{iA}, ileti M ve bu evrede üretilen tek kullanımlık rastgele seçilmiş imza oturum değeri n, yardımıyla önerilen eşleme tabanlı imza şemasıyla oluşturulur. İmza, (S,R) , (3) kullanılarak üretilir.

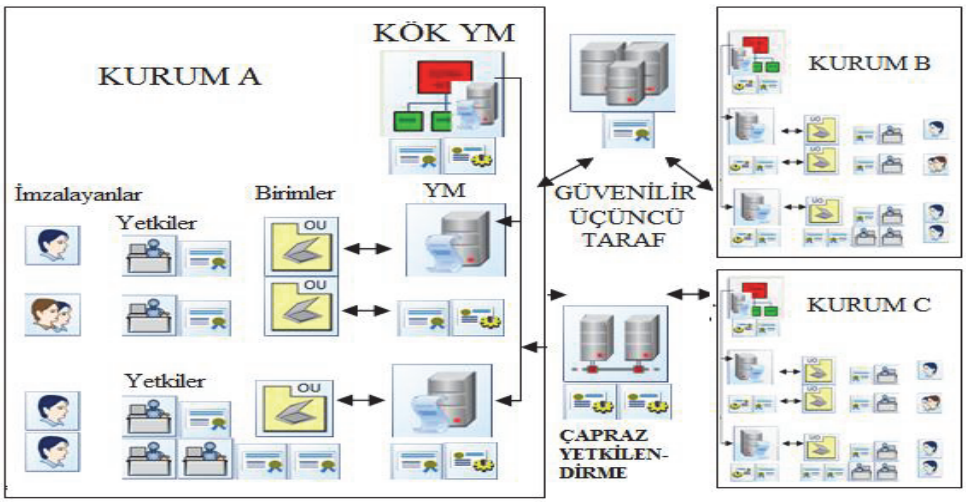
$$R = n.H1(A), r = H2(M,R) \text{ ve } S = (n+r).PR_{iA} \quad (3)$$

Doğrulama sürecinde yetkibilgisi ve yetkili sayısal imza doğrulanır. Doğrulayan taraf öncelikle imzayı açık anahtar ile doğrular. YM'na *yetkibilgisi*nin doğrulanması isteğini gönderir. YM'nda *yetkibilgisi* ve ilişkili yetki konusunu kontrol edilir. Doğrulayan taraf YM'dan aldığı onay cevabına göre imzayı kabul veya reddeder. İmzanın doğrulanması, kriptografik çift doğrusal eşleme özellikleri ile elde edilir. Eğer denklem (4) sağlanıyor ve YM *yetkibilgisi*ni doğrulamışsa yetkili imza doğru ve geçerlidir.

$$e(g,S) = e(PU_i, R + r.H1(A)) \quad (4)$$

4.2 Gerçekleme ve Performans Analizi (Implementation and Performance Analysis)

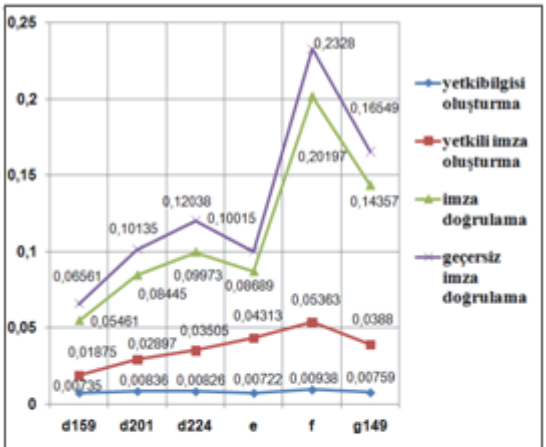
Önerilen yetkili sayısal imzalama modeli, Ubuntu 10.04 işletim sistemi üzerinde, açık kaynak kodlu



Şekil 3. Modelde Yetkilendirme Makamı (Authorization Authority in The Model)

eşleme tabanlı kriptografi ve GMP matematiksel tanım kütüphaneleri [16], [21], [22] 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 5'te sunulmuştur.

Yetkibilgisi 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.

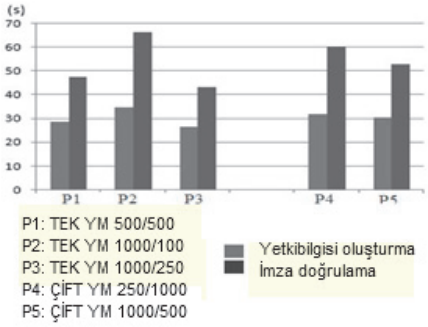


Tip	Alan büyüklüğü	k-eğri derecesi	Dlog güvenlik	Eğri elde yöntemi
d*n*	*n*	6	6*n*	MNT
e	1024	1	1024	CM
f	160	12	1920	Paulo-Barreto.
g*n*	*n*	10	10*n*	Freeman-Scott

Şekil 5. Yetkili sayısal imzanın farklı eğri tipleriyle gerçeklenme performans grafiği (Performance of authorized digital signature implementations with different curve types)

Yapılan diğer performans analizi ile YM üzerindeki yük incelenmiştir. YM'nın *yetkibilgisi*ni üretmesi ve imza doğrulama görevlerini, eş zamanlı çoklu istemcilerden gelen istekler karşısında gerçeklemesi esnasındaki performansı incelendiğinde Şekil 6'da sunulduğu gibi imza doğrulama isteği sayısı 1000 ve üzerine ulaştığında, ortalama cevaplanma süresi 1 dk'nın üzerine çıkabilmektedir.

Performans çözümleri için, önerilen çok katmanlı YM modeli ile gelen istekler farklı YM'na dağıtılarak performans istenen seviyeye çekilebilinir. Modelde gizli ve açık imza anahtar ikilisini üreten birim ile YM'nın aynı birim olması zorunluluğu yoktur. Çünkü Yetkibilgisi ile hazırlanan yetkili imza anahtarı ile üretilen imza, var olan açık anahtar ile doğrulanabilmektedir.



Şekil 6. Yetkilendirme Makamı yetkibilgisi üretme ve doğrulama performans değerleri (AA authorization information generation and verification performance values)

Önerilen çalışma yetkinin denetimi için yetkibilgisine 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 (Reliability and system security analysis)

Çalışmada yapılan erişilebilirlik analizi, iş akışındaki tetikleme ve çakışıklık matrisleri ile hesaplanmış ve doğrulamada petri ağı performans ve güvenilirlik analizi aracı PIPE [23], [24]'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 [3], [25]. 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'nın aynı birim olma gereksinimi yoktur. Böylelikle YM, kullanıcı u_a'ya ait gizli anahtarı bilmediğinden, *yetkibilgisi*ni 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. *Yetkibilgisi* sahip olunan kişiye aitlik ve YM'nın onayını taşıma özelliklerine sahip olduğundan; üçüncü taraf, başkasının *yetkibilgisi* ve kendi imza anahtarıyla

geçerli yetkili imza üretemez veya bu amaçla sahte *yetkibilgisi* üretemez. *Yetkibilgisi*nin doğru kaynakta üretilip üretilmediği taşıdığı onay imzası ile kontrol edilebilirdir. Bu ve benzeri durumlarda AA'nın doğruluğu sorgulanacaksa *yetkibilgisi*ndeki açık anahtar kullanılmamalıdır. Sunulan şemanın güvenlik analizi takip eden bölümde sunulmuştur.

4.4 İmza şemasının Rastsal Kahin Modeli ile Güvenlik Analizi (Random Oracle Model Security analysis of the signature scheme)

Random Oracle (Rastsal Kahin) Modeli [26] 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)'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 M iletisi, *yetkibilgisi* 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 Özgün Katkılar ve Tartışmalar (Original Contributions and Discussions)

Kerberosun dağıtık sistemlerde yetkilendirme konusundaki eksiklikleri ve güvenlik için yetkilendirme mekanizmasına ihtiyaç duyduğu bilinmektedir [3]. Çalışmada 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[25]. Kullanıcıların genel tanımlarla yapılmış yetki kısıtlamalarını iş akışında atlatarak yetkisiz belge üretimi/onayı yapabildiği erişilebilirlik analizi ile sunulmuştur. Rol tabanlı erişim denetimi yöntemleri, [4], [5] erişim denetim listelerinin yetersizliklerine [25] çözüm olarak önerilmiştir.

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 [6], grup [7], [8] ve kimlik tabanlı [9], [10] 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. SONUÇLAR (CONCLUSIONS)

Bu çalışmada, kurumsal işakışındaki 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 model geliştirilebilir.

SEMBOLLER (NOTATIONS)

(PR_i, PU_i) : i kullanıcısına ait (gizli,açık) imza anahtarı ikilisi
A : yetkibilgisi
PR_{iA} : $e\{PR_{iA}\}$ eşleme fonksiyonu ile üretilen yetkili imza anahtarı
(S, R) : Yetkili Sayısal İmza
$H1: \{0,1\} * -> G, H2: \{0,1\} * X\ G -> Z_q^*$: kriptografik özetleme fonksiyonları

KAYNAKLAR (REFERENCES)

1. Neuman B. Clifford and Ts'o T. "Kerberos: An Authentication Service for Computer Networks", ***IEEE Communications*, 32(9):33-38**, 1994.
2. Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", **RFC 2138,** April 1997.
3. Jie W, Arshad J, Sinnott R, Townend P, and Lei Z. "A review of grid authentication and authorization technologies and support for federated access control." **ACM Computing Surveys,** 43, 2, Article 12, 2011
4. ANSI, American National Standard for Information Technology—Role Based Access Control, p. 359, **ANSI Int'l Committee for Inf. Technology Stds**, 2004
5. Ferraiolo D.F., Kuhn R., Sandhu R., "RBAC Standard Rationale: comments on a Critique of the ANSI Standard on Role Based Access Control", **IEEESecurity Privacy, v5/6**, 2007
6. Mambo M., Usuda K., Okamoto E. "Proxy signatures: Delegation of the power to sign messages", **IEICE Trans. Fundamentals**, Vol. E79-A No. 9, 1996.
7. Chaum D., Heyst E.Van, "Group signatures", **Advances in Cryptology, EUROCRYPT '91**, LNCS Vol. 547,257–265, 1991.
8. Bellare M., Shi H., Zhang C., "Foundations of Group Signatures: The Case of Dynamic Groups. Topics in Cryptology" **CT-RSA 2005 Proc.**, **LNCS** Vol. 3376, 2005
9. Shamir A.,"Id- Based Cryptosystems and Signature Schemes", **LNCS** Vol. 7 1984.
10. Paterson K. G., "ID-based signatures from pairings on elliptic curves", **IEEE Communication Letters**, 38(18), 2002.
11. Vural Y., Sağıroğlu Ş.**,** "Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler", **Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi**, Cilt:26, No:1, 2011.
12. Jensen, K., "Coloured Petri nets. Basic concepts, analysis methods and practical use", **Monographs in Theoretical Computer Science**, vol. 1. Springer, Heidelberg, 1992
13. Al-Azzoni, I., Down, D.G., Khedri, R. "Modelling and verification of cryptographic protocols using coloured Petri nets and Design". **Nordic Journal of Computing 12(**3), 2005
14. Zaitsev, D.A.**, Clans of Petri Nets: Verification of protocols and performance evaluation of networks**, LAP LAMBERT Academic Publ, 2013.
15. Boneh D., Lynn B., Shacham H. "Short signatures from Weil pairing", **LNCS** 2248, 2001.
16. Barreto P.S.L.M "The pairing-based cryptography lounge". **http://www.larc.usp.br/~pbarreto/ pblounge.html,** erişim, 2014.
17. PKI, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", **RFC 5280**,IETF, 2008.
18. Farrell, S.,Housley, R "An Internet Attribute Certificate Profile for Authorization", **RFC 3281**,IETF, 2002.
19. PKI,"Internet X.509 Public Key Infrastructure Profile",**RFC 5280**, IETF, 2008.
20. Joux A., "A one round protocol for tripartite diffie-hellman", **Proc. of the 4th International Symposium on Algorithmic Number Theory**, Springer-Verlag, 2000
21. Pairing-based cryptography library, **http://crypto.stanford.edu/pbc/**, erişim, 2014
22. GMP, "GNU Multi-precision Arithmetic Library", **http:// gmplib.org,** erişim, 2014
23. Dingle N.J., Knottenbelt W.J., Suto T., "PIPE2: A Tool for the Performance Evaluation of Generalised Stochastic Petri Nets (PDF Format).", **ACM SIGMETRICS Performance Evaluation Review (Special Issue on Tools for Computer Performance Modelling and Reliability Analysis)**, Vol. 36(4), pp.34-39. 2009
24. PIPE: Platform Independent Petri net Editor 2, **http://pipe2.sourceforge.net/**, eriş., 2014
25. Barkley J. "Comparing simple role based access control models and access control lists". In **Proceedings of RBAC '97 ACM,** NY, 127-132.,1997
26. Bellare M, Rogaway P., "Random Oracles are practical: A Paradigm for Designing Efficient Protocols", **ACM Conf. Computer and Communication Security**, 1993.