# Akıllı Şehirler için Mahremiyet Yönetimi
# Privacy Management for Smart Cities

Nadin Kökciyan ve Pınar Yolum
Bilgisayar Mühendisliği
Boğaziçi Üniversitesi
Bebek 34342 (İstanbul, Türkiye)
nadin.kokciyan@boun.edu.tr, pinar.yolum@boun.edu.tr

***Özetçe* —Akıllı şehirler, birbirleriyle haberleşen nesneler üzerinden vatandaşlarına faydalı servisler sunmayı hedefliyor. Bunun temel taşı olan, Nesnelerin İnternet'i etrafımızdaki nesnelerin haberleşmesini ve birlikte çalışmasını sağlıyor. Aynı zamanda, nesnelerin, kullanıcıların bilgilerini toplamaları ve işlemeleri, daha önceden alışık olmadığımız mahremiyet ihlallerine yol açıyor. Birçok zaman, bir akıllı şehir servisini kullanan kullanıcı, hangi nesnenin, hangi bilgileri, hangi sebeplerle topladığından haberdar edilmiyor. Bu da mahremiyet yönetimi için sıkça kullanılan mahremiyet sözleşmelerinin, bu tür, paydaşların ve bilgilerin belli olmadığı durumlarda uygulanmalarını son derece zorlaştırıyor. Bu çalışma, akıllı şehir uygulamalarında kullanılmak üzere, nesnelerin İnternet'i için bir mahremiyet yönetim modeli sunmaktadır. Bu model, iyi bilinen *bağlamsal doğruluk* kuramından yola çıkmakta ve bir yapay zeka yöntemi olan muhakeme yöntemiyle hangi durumun mahrem olduğuna karar vermektedir. Bunu yaparken, farklı kaynaklardan gelen bilgilerin farklı güvenilirlikte olduğunu gözönüne almakta ve bilgiler üzerinde muhakeme yaparak sonuca ulaşmaktadır.**

***Anahtar Kelimeler*—Nesnelerin İnternet'i, mahremiyet, muhakeme kuramı**

***Abstract*—Smart cities aim to provide intelligent services to their users through the use of connected entities. Internet of Things is emerging as the backbone to facilitate these services. At the same time, the communication of these entities is making privacy to be violated much easier than before. Many times, it is not clear which entities have access to which information, for which purposes the access is being granted, and so on. A leading approach to manage privacy on the Web is the use of privacy policies. However, since the information that would need to go into a privacy policy is usually not available up front for IoT, privacy policies are difficult to apply. Accordingly, this paper proposes a new computational model for the well-known *contextual integrity* theory for IoT. The proposed model enables IoT entities to reason about the context they are in based on information they gather from different entities in the system using argumentation. The model takes into account that information from different sources will have varying degrees of trustworthiness and that each entity has a different degree of belief in the information it provides.**

***Keywords*—Internet of Things, privacy, argumentation theory**

## I. GİRİŞ

Akıllı şehir vizyonu, birbiriyle haberleşen birçok kişi, etmen veya nesnenin, bilgilerini biraraya getirerek vatandaşlarına hayatı kolaylaştıracak servisler sunmasını içeriyor. Bu servisler, vatandaşların istedikleri yerlere daha kolay ulaşmalarını, daha iyi bir sağlık servisi almalarını ya da önceden tespit edilemeyen atıkların toplanabilmesinden dolayı daha temiz bir şehirde yaşamalarını sağlayabilir. Öte yandan, bahsi geçen nesneler, insanlar hakkında bilgileri çok rahatlıkla, belki insanların haberi bile olmadan toplayabilir. Kendisi hakkında bir bilginin toplandığını bile bilmeyen bir kişi, bu bilginin kimlerle paylaşıldığını, ne için kullanıldığını ise hiç bilemeyebilir. Bunun sonucunda, mahremiyet ihlalleri olması kaçınılmaz olur [8].

Akıllı şehirlerde ortaya çıkabilecek mahremiyet ihlalleri, yazılımlarda sıkça kullanılan erişim kontrol problemlerini andırıyor olsa da, önemli farklılıklar vardır. Geleneksel bir erişim kontrol probleminde, bütün veriyi elinde tutan ve kimin neye erişeceğine karar veren bir yönetici mevcuttur. Bir veriye erişmemesi gereken kişi, veriye erişirse bunun sonucunda bir hata oluşması beklenir. Fakat, Nesnelerin İnternet'i gibi dağıtık modellerde, özellikle nesnelerin farklı kurumlar tarafından yönetildiği durumlarda, böyle bir erişim modelini uygulamak zordur. Her nesne kendi yetilerini kullanarak (ör. fotoğraf çekerek) bir takım bilgilere erişebilir ve hatta bunu diğer nesnelerle paylaşabilir. Bundan doğacak mahremiyet ihlallerini kullanıcıların da sistemin de tespit etmesi çok güç olabilir [6]. Bundan dolayı, ortaya çıkacak mahremiyet durumları üzerinde fikir yürütmek için akıllı, dağıtık, anlamsal yöntemlere ihtiyaç vardır [2].

Ortaya çıkabilecek mahremiyet ihlallerini anlamak için önce mahremiyetin özelliklerini anlamak gereklidir:

*Öznel*: Güvenlikten farklı olarak, mahremiyet kişiden kişiye farklı bir anlam ifade edebilir. Bir kullanıcı, sokakta çekilmiş fotoğraflarının kimse tarafından görülmesini istemezken, bir diğer kullanıcı hangi sokaklardan geçtiğinin bilinmesini istemeyebilir.

*Çıkarımsal*: Mahremiyet ihlali, istenmeyen bir bilginin, istenmeyen kişilere ulaşmasıyla oluşur. Fakat, bu bilgi her zaman ham olarak toplanmış olmayabilir. Hangi sokaklardan geçtiğinin bilinmesini istemeyen bir kişinin geçtiği sokaklar, bir bir kayıt edilmediği halde, elde edilen diğer bilgilerden (ör. kişinin bindiği otobüsün rotasından) çıkarılabilir.

Geleneksel sistemlerde, mahremiyeti yönetmenin en temel yolu, her kişiye mahremiyet isteklerini belirtecek, mahremiyet sözleşmeleri hazırlamaktır. Web sitelerinde kullanılan, doğaldil tabanlı ve herkese aynı uygulanan sözleşmeler yerine, kişilerin kendilerine göre özelleştirdiği, makineler tarafından işlenebilen sözleşmeler mahremiyet için daha uygundur [4]. Fakat, Nesnelerin İnternet'i ortamında, böyle sözleşmeler yapabilmek için birçok önşart gerektiğinden son derece zah-

978-1-5090-6494-6/17/$31.00 

metlidir. Buna alternatif olarak, bir bilginin paylaşılmasına *bağlamsal* olarak karar vermek iyi bir genelleme yöntemidir. Nissenbaum tarafından geliştirilen bağlamsal doğruluk kuramı bunu gerçeklemek için önemli bir altyapı sunmaktadır [7]. Bu kurama göre, her bağlam içinde nelerin yapılıp yapılmayacağının normları vardır. Örneğin, bir hastane bağlamında, doktorun hastasına ağrılarıyla ilgili soru sorması normlara uygunken, hastanın maaşıyla ilgili soru sorması uygun değildir. Benzer şekilde, akıllı trafik planlaması yapan bir servisin, bir caddeden kaç araba geçtiğinin sayması normalken, geçen arabaların plakalarını kaydetmesi normlara uygun değildir. Bu tür normlar, hangi bilgilerin kayıt edilebileceğini söyler. İkinci tür normlar da, kayıt edilen bilgilerin nasıl dağıtılacağı ile ilgilidir. Önceki örnekte, doktorun hastanın ağrılarıyla ilgili aldığı bilgiyi, hemşireyle paylaşması normlara uyarken, eşiyle paylaşması normlara uymaz.

Bu çalışmada, akıllı şehir uygulamalarında kullanılmak üzere Nesnelerin İnternet'i üzerinde çalışan bir mahremiyet yönetim modeli önerilmektedir. Bu modelde, akıllı şehir servisleri için veri toplayan her nesne akıllı bir etmen olarak gösterilmektedir. Her etmen, bir bilgiyi kaydetme veya paylaşma anında, önce içinde bulunduğu bağlam hakkında fikir yürütür, daha sonra bu bağlamın normlarına uygun şekilde hareket ederek mahremiyet ihlallerine yol açmayacak şekilde hareket eder. Bağlam hesaplaması sırasında, değişik kaynaklardan gelen veriler, önce etmenin güven hesaplamalarından geçer. Bu sayede, her nesneye eşit güvenilmediği ortamlarda bile, doğru bilgiler üzerinden hesaplama yapılmış olur.

## II. Problem Tanımı

Nesnelerin İnternet'i dünyasında, akıllı cihazlar birbirleri ile etkileşim halinde bulunmaktadır. İnsanlar, farkında olarak ya da olmayarak nesneler ile etkileşim halindedir. Bunun en sık yaşanan örneği, mekanlara konan kameralardır. İnsanlar mekanlara girip çıkarken, yerleştirilen kameraları farketmeyebilir. Oysaki kameralar sürekli insanların görüntülerini kaydetmektedirler.

**İşlenen Senaryo** Beril'in çalıştığı yerin hemen dışında sürekli çekim yapan bir kamera vardır. Kamera, normal şartlarda bu görüntüleri başka kişilerle paylaşmamaktadır. Beril'in patronu olan Hicran, Beril'in 30 Kasım'da çekilen görüntülerine erişmek istemektedir. Çekim halinde olan kamera, acil bir durum görmediği için bu görüntüleri vermez. Daha sonra, Hicran kamera ile Beril'in kaybolmuş olduğu bilgisini paylaşır. Kamera, Hicran'a çok güvenmediği için söylediğinin doğruluğunu kendi ölçmek ister. Beril'in oturduğu ev sensörü ile iletişime geçer. Acil bir durum olabileceği kaygısına kapılır ama emin olamaz. Kamera, görüntüleri paylaşmamaya devam eder. En sonunda, kamera polis departmanı ile iletişime geçer. Beril hakkında bir kayıp raporu olduğunu öğrenir. Bu bilgiye güvenen kamera, Beril'in acil bir durum içerisinde olduğunu anlar ve görüntüleri paylaşır.

**Biçimsel Tanım** Bu çalışmada, her nesne bir etmen olarak modellenir. Etmenlerin içerisinde bulundukları fiziksel dünyayı anlamaları ve diğer etmenler ile iletişimi kurmaları gerekmektedir. Bunun için biçimsel bir tanım şarttır. Böylece etmenler otomatik olarak kendi kararlarını alabilir.

Yukarıdaki örneklerin betimlenmesinde kullanılacak bir takım özellikler vardır. Her etmen *:etmenadi* olarak tanımlanır. Örneğin, *:kamera*, kamera etmeni gösteriminde kullanılır. *kapsamda*(A, C, T) özelliği, A etmeninin T zamanında C bağlamında olmasını ifade eder. *:iş* iş bağlamı, *:acil* acil durum bağlamı, *:emeklilik* ise emeklilik bağlamını gösterir. *bilgi*(X), etmenin bildiği X bilgisini ifade eder. *işinde*(A, T) özelliği bir A etmeninin T anında işte olduğunu tasvir eder. A etmeninin T anında kayıp olduğu *kayıp*(A, T) ile ifade edilir. *yangın*(T) ise T anında yangın olduğu anlamına gelir. *görüntüPaylaş*(A, T) özelliği T anında A etmenine ait kamera görüntülerinin paylaşılmasını ifade eder. Tüm özelliklerin olumsuz durumları, özelliklerin başına değilleme işareti ($\sim$) getirilerek ifade edilir. $\sim$*izinde*(A, T), A etmeninin T anında izinli olmadığını gösterir. *işgünü*(T), T anının bir iş gününe denk geldiği anlamına gelir. $\sim$*evde*(A, T) ise A etmeninin T anında evde olmadığını tasvir eder.

## III. Yaklaşım

Etmenlerin özerk bir yapıda, kendi kararlarını alabilmeleri için birtakım ihtiyaçlar vardır: (i) Nesnenin, içerisinde yer aldığı ortamın biçimsel olarak modellenmesi şarttır. Böylece, nesne ortamı gözlemleyerek bilgilerini günceller. (ii) Nesne, birtakım kurallar doğrultusunda kendi işleyişini yürütebilmelidir. Bunun yanında, nesnenin mahremiyeti koruyabilmesi için bir mahremiyet modeli tanımlanmalıdır. (iii) Bir nesne sadece kendi bilgilerini değil başka nesnelerden topladığı bilgileri de kullanacaktır. Nesnelerin aralarında anlaşmalarını sağlayacak biçimsel bir dil gereklidir. Çok-etmenli bu sistemde, iletişim kanalları nesneler tarafından karşılıklı benimsenecek protokoller vasıtasıyla yapılmalıdır.

Çok-etmenli sistemlerde, etmenler muhakeme yaparak birbirlerine argümanlar sunarlar, ve argümanlarının doğruluğunu savunmaya çalışırlar. Taraflar birbirlerinin argümanlarını çürütmeye ve birbirlerini ikna etmeye çalışırlar. En iyi argüman bulunmaya çalışılır. Muhakeme yönteminde iki önemli parça vardır: argümanlar ve atak ilişkileri. Bir argümanın diğer bir argümandan kuvvetli olması durumu, ilk argümandan ikinci argümana gelecek bir atak ile mümkündür.

Bu çalışmada, ASPIC [3] muhakeme yöntemi kullanılmaktadır. ASPIC, soyut muhakeme yöntemi üzerine kurulmuştur. ASPIC içerisinde tanımlanması gereken bilgiler ve kurallar vardır. Hem bilgiler, hem de kurallar kesin doğru olmak zorunda değildir. Dolayısıyla, sıfır ile bir arasında değerler verilerek bir bilginin veya kuralın ne kadar inanılır olduğu ifade edilebilir. Muhakemenin yapılabilmesi için mantıksal bir dil seçilmelidir. Bilgiler ve kurallar bu dilin öğelerini kullanarak tasvir edilir. Her kural, $\sigma_1$,...,$\sigma_m \leftarrow \sigma_0$ ($m \geq 0$, $\sigma_i \in \mathcal{L}$) biçimindedir. $\mathcal{L}$ seçilen mantıksal dile, $\sigma_i$ ise bu dilde yer alan haberlere denk gelir.

Burada seçilen dil, aynı zamanda etmenlerin içerisinde bulundukları ortamın tasviri için de kullanılır. Bu dil ile oluşturulan bir protokol vasıtasıyla, etmenler birbirleri ile mesaj alışverişinde bulunur. Bu çalışmada, bir etmen ihtiyaç duyduğu bilgileri başka etmenlere kendi sorar. Protokol kapsamında, soru sorulan etmen bu bilgiyi bilir veya bilmez. Bildiği takdirde, bilgiyi ve bu bilgiye olan inanç değerini soran etmen ile paylaşmalıdır. Etmen, toplanan her bilgiyi değerlendirip kendi karar mekanizmasına dahil edip etmeme kararı almalıdır.

Bu çalışmada, mahremiyet modeli Nissenbaum tarafından önerilen Bağlamsal Doğruluk [7] modeli ile tanımlanmaktadır.

Bu modele göre, farklı tür bağlamlar vardır. Her bağlamın kendine ait normları, ve müsaade ettiği (mahrem olmayan) veri paylaşımları vardır. Bir bilginin mahrem olup olmaması hangi bağlamda ele alındığına ve bu bağlam içerisinde kişilerin rolleri ve yapabildikleri ile değerlendirilmelidir.

Bağlamsal doğruluk teorisi birçok çalışma içerisinde kullanılmıştır. Barth ve arkadaşları mantık tabanlı bir mahremiyet sistemi önermişlerdir [1]. Mahremiyet sözleşmeleri normlardan oluşur, ve her norm zamana bağlı formüller halinde gösterilir. Önerilen model, tek bir organizasyon içerisinde, rollerin çok net olarak belli olduğu zamanlarda kullanılabilir. Krupa ve Vercouter, bağlamsal doğruluk teorisini dağıtık sanal topluluklar içerisinde mahremiyet ihlallerini tespit etmek için kullanmışlardır [5]. Her kullanıcı, mahremiyet sözleşmeleri aracılığı ile uyulması gereken beklentilerini belirtir. Bizim çalışmamız dağıtık bir sistem modeli üzerine kurulmuştur, ve roller yerine ilişkiler kullanılmaktadır. Nesnelerin İnterneti söz konusu olduğu zaman, her insandan mahremiyet sözleşmeleri almak mümkün değildir. Ayrıca, bizim çalışmamız kapsamında bir etmen, birden çok bağlamda yer alabilmektedir.

## IV. NORMLAR

Bağlamsal Doğruluk modeline göre, etmenler bağlama göre tanımlı normlar doğrultusunda hareket etmelidir. Bu çalışmada, normları tanımlarken, ASPIC [3] mekanizmasının olanak sağladığı kuralları ele alıyoruz. Kurallar, sıfır ile bir arasında bir değer alır. Bu değer, bir olduğu takdirde, bu kural *mutlak kural* adını alır. Mutlak kuralları betimlerken, $\leftarrow$ gösterimi kullanılır. Eğer kuralın sahip olduğu değer birden küçük ise, bu kurala *çürütülebilir kural* denir. Çürütülebilir kuralları betimlerken, $\Leftarrow$ gösterimi kullanılır. Önerdiğimiz sistemde, çürütülebilir kurallar aynı değere sahiptir ve bu değer de 0.9 olarak seçilmiştir.

### A. Değerlendirme

Bir sistemin işleyişini normlar sağlar. Tablo I içerisinde, kamera etmenine (*:kamera*) ait normlar gösterilmektedir. Her kural, $R_i$ şeklinde gösterilmiştir ve $i$ değeri de kuralın kaçıncı kural olduğunu göstermektedir. $R_1$ kuralına göre, eğer A etmeni T zamanında işte ise, bu etmenin bağlamı T zamanında *:iş* bağlamıdır. Etmenin içerisinde bulunduğu bağlam, birden fazla farklı şekilde aynı olabilir. Örneğin, $R_2$ ve $R_3$ kuralları iki farklı kuraldır ve iki kuralın sonucunda da etmenin acil bir durumda olduğu anlaşılmaktadır. $R_2$ kuralına göre, eğer A etmeni T anında kayıp ise, bu etmen T anında acil durum (*:acil*) bağlamındadır. $R_3$ kuralında ise, bir etmen iş ortamındayken yangın görülüyorsa, bu etmen acil durum bağlamındadır. $R_4$ ile $R_6$ arasında betimlenen kurallar ise, kamera etmeninin hangi durumlarda bir etmene ait görüntüyü paylaşıp paylaşmayacağına karar verilmesinde rol oynar. Kamera etmeni, başka bir etmene ait görüntüleri, bu etmenin acil bir durum içerisinde olduğunu düşündüğü zamanlarda paylaşabilir ($R_5$). Bu etmen için sürpriz bir emeklilik partisi düzenleneceği zaman da, kamera etmeni bu etmene ait görüntüleri paylaşmak isteyebilir ($R_6$). Fakat, eğer bir etmen iş bağlamı içerisinde bulunuyorsa, kamera etmeni bu etmene ait görüntüleri paylaşmak istemeyebilir ($R_4$). Bir etmenin ne zaman kayıp olduğunun anlaşılması $R_7$ kuralında gösterilmektedir. Eğer A etmeni T zamanında iş gününde izinli değilse ve A etmeni T zamanında evde değil ise, T zamanında A etmeninin kayıp olacağı düşünülebilir.

TABLO I. *:kamera* ETMENINE AIT NORMLAR

| |
|---|
| $R_1$ : *kapsamda*(A, *:iş*, T) $\Leftarrow$ *bilgi*(*işinde*(A, T)). |
| $R_2$ : *kapsamda*(A, *:acil*, T) $\Leftarrow$ *bilgi*(*kayıp*(A, T)). |
| $R_3$ : *kapsamda*(A, *:acil*, T) $\Leftarrow$ *bilgi*(*işinde*(A, T)), *bilgi*(*yangın*(T)). |
| $R_4$ : $\sim$*görüntüPaylaş*(A, T) $\Leftarrow$ *kapsamda*(A, *:iş*, T). |
| $R_5$ : *görüntüPaylaş*(A, T) $\Leftarrow$ *kapsamda*(A, *:acil*, T). |
| $R_6$ : *görüntüPaylaş*(A, T) $\Leftarrow$ *kapsamda*(A, *:emeklilik*, T). |
| $R_7$ : *bilgi*(*kayıp*(A, T)) $\Leftarrow$ *bilgi*($\sim$*izinde*(A, T)), *bilgi*(*işgünü*(T)), *bilgi*($\sim$*evde*(A, T)). |

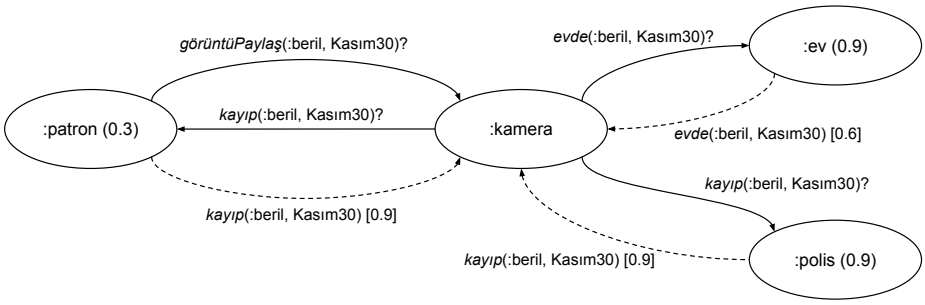
### B. Etmenler Arası Güven Değerlerinin Hesaplanması

Bir etmen, kendine ait bilgileri kullanabilir. Bu bilgiler arasında, kendi normları da yer almaktadır. Çoğu zaman, bir etmenin sahip olduğu bilgiler yetersiz gelebilir ve bu da sağlıklı bir sonuca ulaşmayı engelleyebilir. Bu tip durumlarda, etmenler başka etmenlere danışarak bilgi toplamayı tercih edebilir. Bunu gerçek hayatta insanların karar verme mekanizmasına benzetmek mümkündür. Örneğin, bir kişi karar vermeden başkalarına danışarak daha sağlıklı bir karar vermeyi isteyebilir. Etmenler de danışacakları etmenleri seçmek durumundadır. Önerdiğimiz sistemde, etmenler diğer etmenlere karşı güven değerlerine sahiptir [9]. Diğer bir deyişle, bir etmen başka bir etmene az ya da çok güvenebilir, güven değeri sıfır ile bir arasında bir değerdir. Bu güven değeri doğrultusunda, bir etmen dışardan gelen bir bilgiyi tutabilir veya kendi karar mekanizması dışında tutmayı seçebilir. Bir etmen önce başka bir etmenden bilgi ister. Bilgiyi veren etmen, bilgi ile beraberinde bu bilginin değerini de verir. Örneğin, etmen verdiği bilgiden çok emin olmayabilir ve değer olarak $0.3$ değerini vermiş olabilir. Bilgiyi toplayan etmen, hem etmene duyduğu güven değerini hem de bilginin değerini gözeterek bir hesaplama yapar. Hesaplama sonucunda çıkan değer, etmenin belirlediği sınır değer üzerindeyse, etmen bilgiyi tutma kararı alır.

Bu çalışmada, bir etmen tarafından dışardan gelen bilgi değerlerinin hesaplanması ve bu bilginin karar mekanizmasına dahil edilip edilmemesini *güven normları* vasıtasıyla yani ASPIC kuralları ile yapılmaktadır. Bu kurallar vasıtası ile etmen aldığı bilgiye ne kadar güveneceğini hesaplar. Eğer hesaplanan değer, etmen tarafından belirlenen sınır değer altında kalırsa, alınan bilgi karar mekanizması dışında tutulur. Hesap esnasında iki tür bilgi kullanılır: (i) Bilgi alan etmen, bilgi veren etmene ne kadar güveniyor? (ii) Bilgi veren etmen, verdiği bilgiden ne kadar emin? Bu iki tür bilgi 0 ve 1 arasında bir değer alır. Bu iki tür bilginin çarpımına bakılır ve bu değer, sınır değer üzerinde ise bu bilgi karar mekanizmasına dahil edilir.

## V. İŞLEYİŞ

Şekil 1 içerisinde, örnekte betimlenen dört etmen (*:patron*, *:kamera*, *:ev* ve *:polis*) arasındaki ilişkiler gösterilmiştir. Her etmen ismi sonrasında, *:kamera* etmeni tarafından ilgili etmen için belirlediği güven değeri verilmiştir. Örneğin, *:kamera* etmeni, *:patron* etmenine $0.3$ değerinde güvenmektedir. *:patron*, 30 Kasım'da çekilen Beril'e ait görüntüleri almak istemektedir. *:kamera* mevcut bilgileri ışığında bu isteği değerlendirir. *:kamera* Beril'in ilgili tarihte işte olduğunu düşünmekte ve bu bilgiye değer olarak da $0.8$ vermektedir (*işinde*(*:beril*, Kasım30) [0.8]). $R_1$ kuralına göre, Beril'in iş bağlamında olduğunu düşünmektedir. Dolayısıyla, $R_4$ kuralı doğrultusunda,




Şekil 1. Etmenler arası etkileşimler.

görüntüleri paylaşmaz, fakat başka etmenlerden bilgi toplayarak görüntüleri paylaşmasını gerektirecek bir durum olup olmadığını anlamaya çalışır. *:kamera* etmeni kendi normlarına baktığı zaman, iki durumda görüntüleri paylaşabileceğini bulur. Bir yol, etmenin acil bir durumda olduğunu bulmaktır diğer bir yol ise etmen için bir emeklilik partisi verilmesidir. *:kamera* iş bağlamında çalışan akıllı bir cihaz olduğu için, Beril'in emekliliği söz konusu olsaydı bu durumu bilirdi. Dolayısıyla ilk yoldaki gibi, Beril'in içerisinde bulunduğu durumun acil bir durum olup olmadığını anlaması gerekir. Bu sonuca varmak için kullanılabilecek iki farklı kural vardır: $R_2$ veya $R_3$. $R_3$ kuralını gözardı eder çünkü kameranın gözlemleyebildiği bir yangın durumu yoktur. $R_2$ kuralını kullanabilme amacıyla, *:patron* etmenine Beril'in kayıp olup olmadığını sorar. *:patron* etmeninin verdiği $0.9$ değerindeki bilgiye göre Beril kayıptır. Bu bilgiyi değerlendirmek için, *:kamera* etmeni güven normlarını kullanır. *:kamera* etmenine ait sınır değer $0.7$ değeridir. Ayrıca, *:patron* etmenine fazla güvenmeyen kamera, aldığı bilgi için kendi değerini hesaplar ve sınır değer altında olduğunu görür. Dolayısıyla, bu bilgiyi karar mekanizması dışında tutmaya karar verir. *:kamera* etmeni tarafından kullanılabilecek bilgiler de vardır. Örneğin, kamera 30 Kasım tarihine denk gelen günün bir iş günü olduğu (*işgünü*(Kasım30)) ve bu günde Beril'in izinli olmadığını (∼*izinde*(*:beril*, Kasım30)) bilmektedir. Bu bilgiler ışığında, kamera Beril'in kayıp olduğu çıkarımında bulunabilir ($R_7$). Bunun için, ev etmenine Beril'in o gün evde olup olmadığını sorar. Ev etmeninin verdiği $0.6$ ağırlıklı bilgiye göre, Beril o gün evde değildir. Kamera etmeni, ev etmenine çok güvenmektedir. Ama yine de, bilgi ağırlığını gözeterek değerlendirme yaptığında, bu bilgiyi kendi karar mekanizması dışında tutmaya karar verir. Çünkü kamera etmeninin hesapladığı bilgi değeri, kendi sınır değerinin altında kalır. Son olarak, polis etmeni ile iletişim kurmaya karar verir. Polis etmenini, Beril hakkında bir kayıp raporu olduğunu ve bu bilginin de $0.9$ değerine sahip olduğunu söyler. Kamera etmeni, polis etmenine güvenmektedir ve verdiği bilginin değeri yüksek olduğu için, kameranın hesapladığı bilgi değeri yüksektir. Dolayısıyla, kamera etmeni bu bilgiyi karar mekanizmasına dahil eder. $R_2$ kuralını kullanarak, Beril'in aslında acil bir durum içerisinde olduğu çıkarımını yapar, ve Beril'in görüntülerini paylaşma kararı alınır. Bu örnekte iki önemli nokta vardır:
(i) Etmenler aynı anda birden fazla bağlam içerisinde yer alabilir. Örneğin, Beril hem iş hem de acil durum bağlamındadır. (ii) Normlara göre iki farklı tezat eylemin yapılması gerekebilir. Burada önemli olan, öncelikli olan eylemin gerçeklenmesidir. Örneğin, bir norma göre görüntülerin paylaşılmaması gerekirken bir diğer norma göre görüntüleri paylaşmak gerekir. Görüntüleri paylaşmak öncelikli eylem olarak hesaplandığı için, etmen kararını görüntüleri paylaşmak şeklinde verir.

## VI. SONUÇ

Bu çalışmada, Nesnelerin İnternet'i dünyasında, her nesnenin özerk bir biçimde kendi kararlarını verebilmesi için her nesne bir etmen olarak modellenmiştir. Her etmen, kararlarını bulundukları bağlamın normlarına göre alır. Etmenler tekil kararlar alabilir fakat biz etmenlerin çoklu iletişim sonucu karar almaları üzerine yoğunlaşıyoruz. Etmenler, tanıdık diğer etmenler ile güven değerlerini de gözeterek bilgi alışverişinde bulunurlar. Kendilerine makul gelen bilgileri de kullanarak, karar vermeye çalışırlar. Bağlamsal Doğruluk modeli kullanılarak bir mahremiyet modeli oluşturulmuştur. Bir muhakeme yöntemi olan ASPIC kullanılarak normlar ve bilgiler ifade edilmiştir. Dağıtık çok etmenli bir sistem önerilmiş, etmenlerin güven tabanlı iletişim kurmaları sağlanmıştır. Bir örnek üzerinde, modelin işleyişi gösterilmiştir.

Bir sonraki çalışmamızda, bağlamlar arasındaki ilişkiler incelenecektir. Bir bağlam bir diğer bağlamı içeriyor olabilir. Böylesi bir durumda, bir bağlam bir diğer bağlama ait ilişkileri ve normları otomatik olarak kullanır hale getirilebilir.

## KAYNAKLAR


[1] A. Barth, A. Datta, J.C. Mitchell, and H. Nissenbaum. Privacy and contextual integrity: framework and applications. In *IEEE Symposium on Security and Privacy*, pages 184–198, 2006.

[2] Ricard Fogues, Jose M Such, Agustin Espinosa, and Ana Garcia-Fornes. Open challenges in relationship-based privacy mechanisms for social network services. *International Journal of Human-Computer Interaction*, 31(5):350–370, 2015.

[3] J. Fox, D. Glasspool, D. Grecu, S. Modgil, M. South, and V. Patkar. Argumentation-based inference and decision making–a medical perspective. *IEEE Intelligent Systems*, 22(6):34–41, 2007.

[4] Nadin Kökciyan and Pınar Yolum. Priguard: A semantic approach to detect privacy violations in online social networks. *IEEE Transactions on Knowledge and Data Engineering*, 28(10):2724–2737, 2016.

[5] Yann Krupa and Laurent Vercouter. Handling privacy as contextual integrity in decentralized virtual communities: The privacias framework. *Web Intelligence and Agent Systems: An International Journal*, 10(1):105–116, 2012.

[6] Mainack Mondal, Peter Druschel, Krishna P. Gummadi, and Alan Mislove. Beyond Access Control: Managing Online Privacy via Exposure. In *Proceedings of the Workshop on Useable Security (USEC)*, 2014.

[7] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[8] Gilad Rosner. *Privacy and the Internet of Things*. O'Reilly, 2016.

[9] Murat Sensoy, Jie Zhang, Pınar Yolum, and Robin Cohen. POYRAZ: context-aware service selection under deception. *Computational Intelligence*, 25(4):335–366, 2009.