

Nesnelerin İnterneti ve Güvenli Bir Sağlık Bilgi Modeli Önerisi

Özgü Can*, Emine Sezer, Okan Bursa, Murat Osman Ünalır
Ege Üniversitesi Mühendislik Fakültesi, Bilgisayar Mühendisliği
İzmir, Türkiye

Özet

Nesnelerin İnterneti (Internet of Things - IoT), akıllı nesnelere ve sensör ağlarından oluşan, “tüm” nesnelere birbirine bağlamayı amaçlayan bir ekosistemdir. Sağlık bilgi sistemleri, IoT'nin kullanılabilirliği ve böylece daha etkin çözümler sunabileceği önemli bir uygulama alanıdır. Bu çalışmada sağlık alanı için son yıllarda uygulama alanı hızla genişlemekte olan IoT teknolojilerinin kullanımı incelenmektedir. Bu kapsamda, sağlık alanında medikal cihazların birer IoT nesnesi olarak düşünülerek, sağlık bilgisinin sistemler arasında değişiminin anlamsal web teknolojileri ile desteklenerek güvenli bir şekilde gerçekleştirilmesi üzerine bir sistem modeli önerilmektedir. Bu modelde, verinin tanımı için alan ontolojilerinin kullanılması planlanmaktadır. IoT cihazlarından başlamak üzere verinin aktarıldığı her noktada hasta mahremiyetinin sağlanması için güvenlik politikalarının tanımlanmasında da anlamsal web teknolojilerinin kullanılması hedeflenmektedir.

Anahtar Kelimeler: IoT, Nesnelerin İnterneti, Anlamsal Web, Sağlık Bilgi Sistemleri, Ontoloji

Abstract

IoT (Internet of Things) is an ecosystem that aims to link all smart objects and sensors to share data. Health information systems are one of the important application domain where IoT technologies can be implemented and so that, more effective solutions can be provided. In this study, the usage of IoT technologies, that has expanded rapidly in recent years, in health domain are examined. In this context, as the medical tools are accepted as IoT an information system model for health domain, which is supported with semantic web technologies to exchange data between systems and services safely, is proposed. In the proposed model, it is planned to use the domain ontologies for defining the health data. It is aimed to describe security policies, which define the access rules and provide privacy, as ontologies. It is also aimed to use semantic web technologies for defining security policies to ensure patient privacy at the each point with the beginning from IoT devices where data is transferred.

Key words: IoT, Internet of Things, Semantic Web, Health Information Systems, Ontology

1. Giriş

İnternet teknolojileri, günümüzde kullanıcıların veriye her an ve her yerden ulaşabilmelerine imkan vermektedir. Bilgi ve iletişim teknolojilerindeki gelişmeler ile kullanıcı ve bilgisayar sistemleri arasındaki etkileşimin hızla artması, akıllı ekosistemlere olan ihtiyacı ortaya çıkarmıştır. Bu ekosistemlerden biri olan Nesnelerin İnterneti (Internet of Things - IoT), akıllı nesnelere ve sensör ağlarından oluşan, “tüm” nesnelere birbirine bağlamayı amaçlayan bir sistemdir. Böylelikle; nesnelerin akıllı, programlanabilir, insanlar ve diğer nesnelere ile etkileşimde olmaları

*Sorumlu Yazar: Özgü Can Adres: Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 35100, Bornova/İzmir TÜRKİYE. E-posta: ozgu.can@ege.edu.tr, Telefon +902323115332

beklenmektedir.

Verinin toplanıp karşılıklı olarak değiştirilebildiği bir sistem olan IoT, kullanıcılar için farklı birçok olanak sunmaktadır. Her an her yerden herhangi bir verinin alınabilmesi, gerçek-zamanlı ya da zaman içerisinde farklı verilerin toplanıp analiz edilebilmesi sağlanabilmektedir. Sensör ağları, akıllı trafik sistemleri, filo yönetimi, akıllı şehirler ve akıllı ev sistemleri IoT'nin başarı ile kullanılmaya başlandığı ilk örneklerdir.

Sağlık bilgi sistemleri, IoT'nin kullanılabileceği ve böylece daha etkin çözümler sunabileceği önemli bir uygulama alanıdır. Sağlık bilgi sistemleri; elektronik sağlık kayıtlarını, teletıp cihazlarını, mobil sağlık (mhealth) uygulamalarını içeren geniş bir alandır. Hasta verilerinin farklı cihazlardan toplanarak analiz edilmesi sonucunda, kronik hastalıkların takip edilmesi, yaşlı bakımının sağlanabilmesi, sağlıklı yaşam (fitness) ve hareketlilik programlarının sürdürülebilmesi ve izlenebilmesi ile uzaktan hasta gözlemesi etkinlikleri dinamik bir şekilde gerçekleştirilebilecektir. Tedavi ve ilaç takibinin etkin bir şekilde gerçekleştirilebilmesi için kullanılan tıbbi cihazlar ve sensörler de IoT sisteminin nesnelere oluşturmaktadır. Örneğin; tansiyon aleti, ateş ölçer ya da kalp atışı sensörlerinden toplanan veriler, hastanın sağlık durumunun izlenmesi için kullanılabilmektedir. Toplanan bu sağlık verilerinin saklanması, sorgulanması, belirli kurallar dahilinde analiz edilmesi ve gerekli durumlar için alarmların tanımlanabilmesi, bireysel sağlık hizmetlerinde özellikle zaman açısından önemli kazanımlar sağlayacağı için, gerekmektedir. Bu kapsamda; ilgili terminolojide tutarlılığın sağlanması, verinin farklı cihazlar arasında paylaşılmasının sağlanması, bu paylaşım sırasında veri güvenliğinin ve kullanıcı mahremiyetinin korunması gerekmektedir.

Bu çalışmada sağlık alanı için son yıllarda uygulama alanı hızla genişlemekte olan IoT teknolojilerinin kullanımı incelenmektedir. Ayrıca, IoT nesnelere gelecek veri akışı da göz önünde bulundurularak, güvenlik ve gizliliğin önemi vurgulanmaktadır. Sağlık alanında veri güvenliğinin ve hasta mahremiyetinin korunması gerekliliği göz önüne alındığında, IoT nesnelere alınacak verilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanabilmesi için sağlık uygulamalarında güvenliği garantileyen bir IoT mimarisi sunulmaktadır. Bu kapsamda, nesnelere birlikte çalışılabilirliğini sağlayacak bir Anlamsal Web teknolojileri tabanlı IoT mimarisi geliştirimi önerilmektedir.

Çalışmanın organizasyonu şu şekildedir: ikinci bölümde IoT, sağlık uygulamaları ve güvenlik kavramları incelenmekte, üçüncü bölümde Anlamsal Web tabanlı güvenli sağlık uygulamaları için bir IoT mimarisi önerilmekte ve dördüncü bölümde gelecek çalışmalar sunulmaktadır.

2. IoT, Sağlık Uygulamaları Ve Güvenlik

IoT, herhangi bir kişinin, herhangi bir şeyin, herhangi bir zamanda, herhangi bir yerde, herhangi bir hizmet ve herhangi bir ağ ile birbirleri ile bağlanmış olduğu bir kümeye yansıtan bir kavram olarak tanımlanabilmektedir. IoT, bütün iş dünyasını etkileyebilecek gelecek nesil teknolojilerde yeni bir yaklaşımdır ve günümüzdeki internet altyapısına akıllı cihazların ve nesnelere tek tek tanımlanarak, bu cihazların birbiri ile bağlantılı olması şeklinde ifade edilmektedir. Böylelikle,

makineden makineye (M2M) senaryoları sağlayacak şekilde cihazların, sistemlerin ve servislerin birbirleri ile ileri düzeyde bağlantılı olması sağlanarak daha fazla fayda sağlanması amaçlanmaktadır [1]. Bu nedenle, otomasyon ile ilgili her alanda IoT'den bahsedilebilmektedir. IoT platformu; akıllı şehirler, trafik sıkışıklığı, atık yönetimi, yapısal sağlık, güvenlik ve acil servisler, lojistik, perakende satış, endüstriyel kontrol gibi oldukça geniş ve farklı bir uygulama yelpazesi için uygun çözümler sunmaktadır [1, 2, 3, 4, 5].

Sağlık alanı, IoT için en çok dikkat çeken uygulama alanlarından biridir [6]. Uzaktan sağlık izleme, spor programları, kronik hastalıklar ve yaşlı bakımı gibi birçok sağlık uygulamasına IoT'nin sunulan hizmetlere artı bir değer katması beklenmektedir.

IoT teknolojilerinden, her bir hizmetinin farklı sağlık çözümleri sunduğu farklı sağlık hizmetlerini destekleyecek şekilde uygulanabilmesi beklenmektedir. Sağlık alanı kapsamında IoT servislerinin tanımı için günümüzde henüz her hangi bir standart bulunmamaktadır. Ancak, bir servisin belirli bir çözüm veya uygulamadan nesnel olarak ayrı tutulamayacağı bazı durumlar olabilmektedir. Bu nedenle; bir servis, yapısı gereği bir ölçüde geneldir ve bazı çözümler ve uygulamalar için yapı taşı olabilecek potansiyele sahiptir. Ayrıca, IoT çatıları için gerekli olan genel servis ve protokollere sağlık alanındaki senaryolarda uygun işlevsellikte olabilmeleri için bazı değişiklikler yapılması gerekebilmektedir. Bunlar; bildirim servisleri, kaynak paylaşma servisleri, internet servisleri, heterojen aletler için çapraz bağlantı protokolleri ve ana bağlantı için link (bağ) protokollerini içermektedir. Bu listeye kolay, hızlı, güvenli ve düşük güç gerektiren aletler ve servisler eklenebilmektedir [7].

Dağıtık ortamlarda bulunan yüksek düzeyde yapılandırılmış ve zengin anlamsallığı olan klinik bilgiyi elektronik sistemler üzerinden kullanabilmek ve paylaşabilmek, son yıllarda bilgi teknolojilerinin sağlık alanındaki çalışmalarının odak noktası olmuştur. Veri standartları, bilgiyi kayıt altına almak için üzerinde anlaşılmaya varılan, ortak ve tutarlı bir yoldur. Belirli bir standart ile modellenen veri, farklı sistemler arasında iletilebilir ve o veri için sistemden sisteme, programdan programa ve kurumdan kuruma aynı anlama sahip olması sağlanabilmektedir. Veri standartları bilgisayarların genellikle aynı anlamda ve yapıda veriyi göndermelerini ve almalarını sağlamaktadır. Yeni bir yapıya çevirmeye gerek kalmaksızın aynı anlamı taşıyan verinin bir bilgi sisteminden başka bir bilgi sistemine aktarılabilmesi birlikte çalışabilirliği sağlamaktadır.

Sağlık alanında günümüzde kullanılmakta olan yaklaşık 2100 farklı standart bulunmaktadır [8]. Bu sayı özel gereksinimleri karşılamak için bile standartların oluşturulduğunun göstergesidir. Bu sayıyı sağlık kuruluşlarının, halk sağlık kurumlarının üzerinde mantıklı bir şekilde çalışabileceği sayıya düşürmek ulusal çalışmaların merkezindedir.

ICD (The International Classification of Diseases - Uluslararası Hastalık Sınıflandırması) [9]; epidemiyoloji, sağlık yönetimi ve klinik amaçlar için standart bir tanı aracıdır. Nüfus gruplarının genel sağlık durumlarının çözümlenmelerini içeren ICD, hastalıkların ve diğer sağlık sorunlarının görülme sıklığını ve yaygınlığını izlemek için kullanılmaktadır. ICD, ölüm belgeleri ve sağlık kayıtları dahil olmak üzere, bir çok farklı sağlık ve nüfus kayıtlarının üzerinden hastalıkları ve diğer sağlık sorunlarını sınıflandırmaktadır. Bu kayıtlar; klinik, epidemiyolojik ve nitelik amaçlı depolama ve teşhis bilgilerinin alınmasını sağlamanın yanı sıra, Dünya Sağlık Örgütü'ne üye

devletler tarafından ulusal ölüm ve kalıcı engellerin istatistiklerinin derlenmesi için temel oluşturmaktadır. Böylelikle; bu kayıtlar, ülkeler tarafından geri ödeme ve kaynak tahsisine karar vermek için de kullanılmaktadır. Bütçe Uygulama Talimatı'na göre; 01.07.2005 tarihinden itibaren hastalıkların ve sağlıkla ilgili sorunların uluslararası istatistiksel sınıflaması olarak kullanılan ICD 10 standardında yer alan Hastalık Sınıf Adı ile Hastalık Kodu'nun faturalarda bulundurulması zorunluluğu getirilmiştir [10].

USVS (Ulusal Sağlık Veri Seti) [11], sağlık alanındaki bütün paydaşların aynı kavramdan aynı içeriği anlamalarını sağlayacak bir terminoloji birliği oluşturmak amacıyla geliştirilmiştir. Veri sözlüğü, sağlık kurumlarından verilerin belirlenmiş standartlar doğrultusunda toplanmasını, çözümünü ve değerlendirilmesini sağlayacaktır. Aynı zamanda, sahadan sağlık verisi toplama konusunda verimi artıracak, tekrarlanan ve hatalı verileri azaltacak ve toplanan verinin amacına daha uygun bir şekilde kullanılmasına imkân tanıyacaktır. USVS, Türkiye'deki sağlık kurumlarında kullanılmakta olan bilgi sistemlerinin referans olarak kullanılacağı bir sözlük çalışmasıdır. Sözlük, farklı kategorilerde veri kümelerinin olduğu sıradüzensel terim ve nesnelere toplulukları ve bu terimler arası ilişkilerden oluşmaktadır. Bununla birlikte USVS, bir veri sözlüğü niteliği taşımayan; ancak Sağlık Kodlama Referans Sunucusu (SKRS) bünyesinde yer alacak ve yine ülke çapında referans olarak kullanılacak olan kodlama ve sınıflandırma sistemlerinin temel tanımlarını da barındırmakta ve bu kodların kullanıldığı veri alanlarını adreslendirmektedir.

Büyük miktardaki sağlık verisini ve bilgisini paylaşmak için Anlamsal Web teknolojilerinin ve ontolojilerinin kullanımı günümüzde bilgi teknolojileri tarafından yaygın olarak kabul edilmiştir [12]. Tıbbi ontolojilerin ve Anlamsal Web teknolojilerinin geniş potansiyeli, IoT tabanlı sağlık uygulamaları tasarımcıları tarafından da yakın ilgi görmektedir. Ayrı bir hizmeti çağırarak için IoT üstüne tıbbi anlamsallığı ve ontolojileri yerleştirmek anlamsal medikal erişim (SMA – Semantic Medical Access) olarak adlandırılmaktadır [7]. [13]'de IoT algılayıcılara dayalı bir anlamsal tıbbi erişim sistemi önerilmiştir. Bu sistemde, IoT sağlık uygulamaları bulutta saklanmakta olan algılayıcı verisinin büyük miktarını analiz etmek için sağlık alanı için tanımlanmış kural motorlarını kullanması önerilmektedir. [14] ve [15]'de acil sağlık hizmetleri için IoT verisini toplayacak, entegre edecek ve birlikte çalıştırabilecek bir veri erişim metodu sunulmaktadır. [16], [17] ve [18] çalışmalarında, IoT ortamı kapsamında sağlık alanı için Anlamsal Web teknolojileri ile desteklenen çalışmalar sunulmaktadır.

IoT'de, kişisel verilerin toplanması ve kullanılması kapsamında kişisel mahremiyetin sağlanması ile ilgili olarak çeşitli zorluklarla karşılaşmaktadır. Bu kapsamda, [19] çalışmada IoT'de veri toplanması sırasında karşılaşılan kişisel mahremiyetin korunması ile ilgili bir literatür çalışması sunulmakta ve mahremiyet esasları “Avustralya Mahremiyet Prensipleri” kapsamında incelenmektedir. [20] çalışmada geleneksel güvenlik çözümlerinin IoT teknolojilerine uygulanamayacağı belirtilmekte, IoT ağında yer alan kullanıcılar ve nesnelere arasındaki veri gizliliğinin, erişim denetiminin ve yetkilendirmenin sağlanması, güvenlik ve gizlilik politikalarının uygulanması gerekliliği açıklanmakta ve bu dinamik yapı içerisinde karşılaşılabilecek güvenlik tehditlerine yönelik çözümler sunulmaktadır. IoT dağıtık yapısının özelliklerinin açıklandığı ve bu kapsamda güvenlik ile ilgili karşılaşılan zorlukların analiz edildiği bir çalışma [21]'de detaylandırılmaktadır. IoT-tabanlı dağıtık sağlık uygulamalara yönelik bir sağlık izleme sistemi için önerilen kimlik denetleme ve yetkilendirme mimarisi [22] çalışmada sunulmaktadır. [23]

çalışmasında, IoT kapsamındaki sağlık uygulamalarında güvenliğin sağlanması için bir anahtar yönetim protokolü önerisi yer almaktadır.

IoT alanında gerçekleştirilen çalışmaların büyük bir kısmı verilerin toplanması ve ayıklanması üzerine olmaktadır. Verinin toplanmasında henüz bir standartlaşmaya gidilmemiştir. Bu çalışmada anlamsal web teknolojilerinin kullanılmasının başlıca nedeni, verinin makineler arasında anlamını diğer bir deyişle bilgiyi paylaşma hedefidir. IoT tabanlı sağlık bilgi sistemlerinde, verinin ontolojik olarak gösterimi hem sistemin insan kullanıcıları hem de makineler ve sistemler arasında birlikte çalışabilirliği ve dolayısıyla yeniden kullanımı arttıracaktır. IoT tabanlı sağlık bilgi sistemlerinde, veri güvenliğini sağlarken kullanıcı mahremiyetinin de korunarak kişiselleştirilmiş güvenlik tercihlerinin uygulandığı bir çalışma ile karşılaşılmamıştır. Ayrıca, veri güvenliğinin ve veri kalitesinin sağlanmasına yönelik çalışmaların yetersiz olması nedeni ile bu kapsamda yapacağımız çalışmalar da ilgili alana önemli katkılarda bulunacaktır.

3. Anlamsal Web Tabanlı Güvenli Sağlık Uygulamaları için IoT Mimari Önerisi

Anlamsal Web’de verinin iyi tanımlanmış anlamı ve diğer veriler ile ilişkileri verilerek bir bilgi ağı oluşturulmakta ve bu bilgi ağı kullanılarak, insanların ve bilgisayarların işbirliği içerisinde çalışması hedeflenmektedir [24]. Bu birlikte çalışabilirliğin sağlanabilmesi için, bilginin anlamının sistem tarafından anlaşılabilir olması gerekmektedir. Bu nedenle, bilgi sistemlerinin geliştirilmesinde, bilginin tanımlandığı ontolojiler önemli bir yere sahiptir. Ontoloji, kavramsallaştırılmış bir söz varlığının [25] makinenin işleyebileceği bir biçimde sunulmasını sağlamakta, kavramların tanımları ile bu kavramların birlikte etki alanı üzerinde bir yapı oluşturmak için birbirleri ile nasıl ilişkili olduklarını ve terimler arasındaki olası yorumları kısıtlayarak belirtmektedir [26]. Verilen bir etki alanında, o alana ait bilgiyi temsil eden ontolojiler birlikte çalışılabilirliği sağlamaktadır. Sağlık alanında çok büyük miktarda bilgi ve veri bulunmaktadır. Sağlık verisinin çeşitli amaçlar için tekrar kullanımının sağlanabilmesi için paylaşılması gerekmektedir. Bu amaçla, ontolojiler birçok sistem tarafından ortak bir çatı olarak kullanılmaktadır.

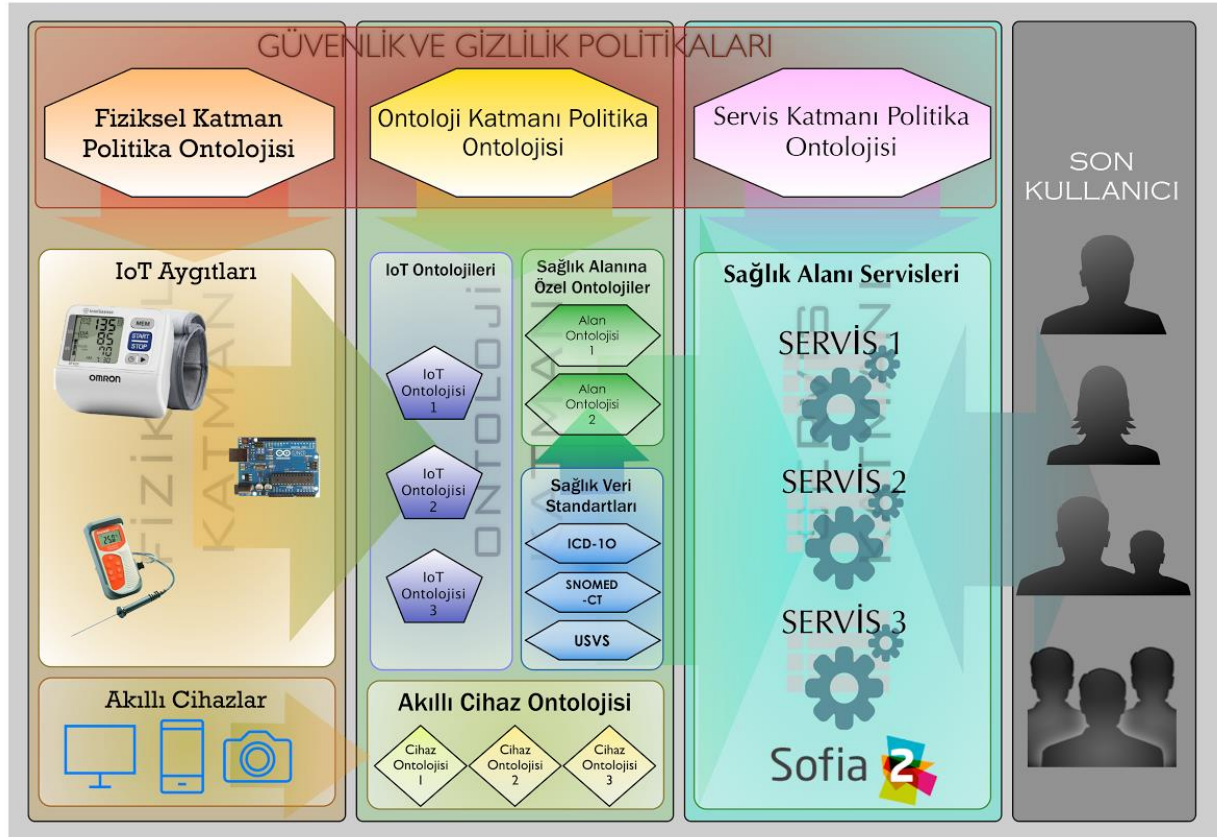
Sağlık verisinin çeşitli uygulamalar tarafından paylaşılması sağlanırken bu paylaşımın veri güvenliği ve kullanıcı mahremiyeti sağlanmış bir şekilde gerçekleştirilmesi gerekmektedir. Sağlık cihazlarına ve uygulamalarına her an ve her yerden bağlanmanın mümkün olması sonucunda, IoT sağlık alanı saldırılara açık bir duruma gelmekte ve bunun sonucunda da kişisel sağlık verisinin korunması önemli bir problem olarak ortaya çıkmaktadır.

Gizlilik, bütünlük, kullanılabilirlik, güven, kimlik doğrulama ve yetkilendirme IoT tabanlı sağlık alanı çözümlerinde dikkat edilmesi gereken temel güvenlik kavramlarıdır. Bu kapsamda; yetkilendirilmemiş kişilerin kişisel sağlık verisine erişiminin engellenmesi, sağlık verisi üzerinde yetkilendirilmemiş değişikliklerin önlenmesi, IoT servislerinin yetkilendirilmiş kişiler, servisler ve ya cihazlar tarafından kullanılabilmesinin garantilenmesi, IoT cihazının iletişimde bulunduğu varlığın kimliğinin doğrulanması ve sadece yetkili varlıkların servislere ve veriye erişebileceğinin sağlanması gerekmektedir.

IoT günümüzde bilişim uygulamalarında bilginin kesintisiz ve doğru olarak her noktadan paylaşılabilmesi için, gelecek nesil internet uygulamalarının en popüler eğilimidir. Bu kapsamda

mevcut uygulamalar oldukça yenidir. Sağlık alanı, oldukça büyük veri barındıran ve kişiye özgü hizmetlerin sunulması gereken bir alandır. Bu nedenle; kişilerin evlerinde rahatlıkla kullandıkları tansiyon, şeker ölçümü, oksimetre, nabız gibi medikal cihazlarda üretilen sağlık verisinin, IoT platformunda toplanarak, kayıt altına alınacağı bir sistemin oluşturulmasına başlanmıştır. Burada hedeflenen medikal cihazdan akıllı cihaza, akıllı cihazdan da buluta aktarımın veri güvenliği sağlanmış bir biçimde gerçekleştirilmesidir. Bu verilerin analizinin yapılması için kurallar geliştirilecektir. Böylece alınan verilerde herhangi bir istenmeyen durum söz konusu olduğunda, bireyin kendisi ve/ya bireyden sorumlu sağlık çalışanı ve/ya sağlık kurumu sistem üzerinden uyarılacaktır.

Her bir uygulamanın ölüm ya da kalıtsal sakatlıklara yol açabileceği düşünülürse verilerin en doğru şekilde alınması, bu verilerin doğru ve hasta mahremiyeti göz önünde bulundurularak saklanması ve bu veriler üzerinden gerekli analizlerin yapılarak sağlık personeli ya da sağlık kurumu tarafından doğru bir şekilde izlenerek, acil durumlarda olabilecek en hızlı ve etkin şekilde müdahale edilebilmesi oldukça önemlidir.



Şekil 1. Sağlık Alanında IoT için Bilgi Sistem Modeli

Şekil 1’de sağlık alanı için IoT nesnelerinin kullanımını destekleyen, güvenilir bir sağlık bilgi sistemi modeli gösterilmektedir. Hızla gelişen teknoloji ile günümüzde birçok kişinin evinde ya da işyerinde tansiyon ölçer, ateş ölçer ve şeker ölçer gibi küçük ve pratik tıbbi cihazlar bulunmaktadır.

Bu cihazlardan elde edilen sađlık verisinin herkesin kullandığı mobil telefon, tablet veya akıllı cihazlara aktarılması ile veri İ nternet altyapısını kullanarak istenilen ortama aktarılabilir.

Verinin sistemden sisteme anlamını yitirmeden aktarılabilmesi için sađlık alanına ait geliştirilecek ontolojilerin kullanılması önerilmektedir. Ayrıca farklı sađlık bilgi sistemleri arasında da verinin paylaşılabilmesi bir diğ er deyiş ile yeniden kullanılabilmesi için sađlık alanında kullanılan standartların da bu ontolojiler tarafından desteklenmesi gerektiğı düşünölmektedir. Verinin akıllı cihazlar ile buluta aktarıldıktan sonra, anlamsal web teknolojilerinin sunduđu çıkarsama ve kural motorları kullanarak gerekli servisler tarafından işlenerek, kişiye, sađlık kurumuna veya sađlık personeline sunulması düşünölmektedir. Verinin toplanması, iletilmesi, işlenmesi ve nihayetinde son kullanıcıya aktarımı süresince sađlık verisinde kişisel mahremiyetin sađlanması bir zorunluluktur. Bu nedenle medikal cihazlardan verinin alınmasından son kullanıcıya iletilmesine kadar tüm süreçte gizlilik ve güvenlik tanımlanan politika ontolojileri ile desteklenmektedir. Sadece yetkilendirilmiş kullanıcıların, cihazların ve servislerin sađlık verisine erişimi güvenlik politikaları üzerinden tanımlanan kurallar ile gerçekleştirilmektedir.

4. Sonuçlar ve Gelecek Çalışmalar

Bu çalışma kapsamında; öncelikle nesnelerin interneti platformunda kişisel sađlık verisinin kayıt altına alınması, sorgulanması ve izlenmesi için sistem tarafından izlenecek sađlık verilerinin ve bu verileri sađlayacak cihazların da yer aldığı güvenlik politikaları ile desteklenen bir bilgi sistemi modeli önerilmektedir. Bu modelde toplanan sađlık verisinin sadece üretildiğı nokta olan medikal cihaz ya da sađlık kliniğinde deđil, gereken her noktada yetkilendirilmiş servis, cihaz ve kişiler tarafından kullanılabilmesi için yeniden kullanılabilirliđin ve birlikte çalışabilirliđin anlamsal web teknolojileri ile sađlanması önerilmektedir.

Önerilen modelin uygulanması için öncelikle sađlık alanı için bir uygulama alanı belirlenecek ve bu alanda kullanılan medikal cihazlar IoT nesneleri olarak seçilecektir. Belirlenen veriler ve cihazlar için birlikte çalışabilirlik ve yeniden kullanılabilirlik hedefleri ile gerekli IoT cihaz ontolojileri ve sađlık alanına özgü ontolojiler geliştirilerek, Sofia2 platformu ile entegre edilecektir. Sofia2 (Smart Objects for Intelligent Applications) platformu, Nokia, Philips, Fiat ve Acciona gibi şirketlerin de yer aldığı Avrupa Birliđi ölkelerinden 19 paydaşın bulunduđu bir R&D Artemis projesi olarak geliştirilmiştir [27]. IoT çalışmalarında yaygın olarak kullanılması, Eclipse platformu üzerinde çalışılabilmesi ve açık kaynaklı bir platform olması nedeni ile Sofia2 platformunun çalışmamızda kullanılması planlanmaktadır. Sofia2 platformu, farklı cihazlar ve sistemler arasında sorunsuz birlikte çalışabilirliđi sađlayan bir katman olarak tanımlanmaktadır. Cihazlardan gelen veriler geliştirilen ontolojilere göre Sofia2 platformunun sunduđu büyük veri saklama desteđi kullanılarak depolanacaktır. Erişim denetiminin, veri güvenliđinin ve mahremiyetin sađlanması için gerekli politika ontolojileri geliştirilecek sisteme dahil edilecektir. Aynı zamanda, kullanıcılar da kişisel mahremiyetlerini ve sađlık verilerinin güvenliđini korumak için güvenlik tercihlerini belirleyebileceklerdir. Veri güvenliđini sađlarken veri analizlerinin başarıya ulaşabilmesinin önüne geçmemek için, veri kalitesi parametreleri belirlenmesine yönelik çalışmalar gerçekleştirilecektir.

Kaynaklar

- [1] Höller J, Tsiatsis V, Mulligan C, Karnouskos S, Avesand S and Boyle D. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Amsterdam, The Netherlands: Elsevier, 2014.
- [2] Kortuem G, Kawsar F, Fitton D, and Sundramoorthy V. Smart objects as building blocks for the Internet of Things. *IEEE Internet Computing*, 14(1), 2010; pp. 44-51.
- [3] Romer K, Ostermaier B, Mattern F, Fahrmaier M, and Kellerer W. Real-time search for real-world entities: A survey. In *Proc. IEEE*, 98(11), 2010; pp.1887-1902.
- [4] Guinard D, Trifa V, and Wilde E. A resource oriented architecture for the Web of Thing. In *Proc. Internet Things (IOT)*, 2010; pp.1-8.
- [5] Tan L, and Wang N. Future Internet: The Internet of Things. In *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, Vol. 5., 201; pp. 375-380.
- [6] Pang Z. Technologies and architectures of the Internet-of-Things (IoT) for health and well-being. M.S. thesis, Dept. Electron. Comput. Syst., KTH-Roy. Inst. Technol., Stockholm, Sweden, 2013.
- [7] Islam SMR, Kwak D, Kabir MDH, Hossain M and Kwak KS. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, Vol. 3, 2015; pp. 678-704.
- [8] MN-PHIN Steering Committee. Public Health Data Standarts, Improving How Public Health Collects, Exchanges and Uses Data. <http://www.health.state.mn.us/ehealth/mnphin/standardards.pdf>, Son Erişim: Ağustos 2016.
- [9] ICD (The International Classification of Diseases) <http://www.who.int/classifications/icd/en/>, 2006; Son Erişim: Ağustos 2016.
- [10] Kaptanoğlu YA. Birinci Basamak ve Yataklı Kamu Sağlık Kurumlarının Gelirlerinden Yapılan Ödemelerde Performans Yönetimi Kavramı. *Yükseköğretim ve Bilim Dergisi*, Cilt 1, Sayı 3, 2011; s.142-151.
- [11] T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı. SağlıkNET Entegrasyonu için Hastane Bilgi Sistemlerinin Temel Gereksinimleri. Ankara, 2007; s. 25.
- [12] Burgun A, Botti G, Fieschi M and Le Beux P. Sharing knowledge in medicine: Semantic and ontologic facets of medical concepts. In *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Vol. 6, 1999; pp. 300-305.
- [13] Zhang G, Li C, Zhang Y, Xing C and Yang J. SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors. In *Proc. IEEE Int. Conf. eHealth Netw., Appl. Services (Healthcom)*, 2012; pp. 238-243.

- [14] Xu B, Xu LD, Cai H, Xie C, Hu J and Bu F. Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Trans. Ind. Informat.*, 10(2), 2014; pp.1578-1586.
- [15] Miori V and Russo D. Anticipating health hazards through an ontology-based, IoT domotic environment. In *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, 2012; pp.745-750.
- [16] Jara AJ, Zamora-Izquierdo MA and Skarmeta AF. Interconnection framework for mHealth and remote monitoring based on the Internet of Things. *IEEE J. Sel. Areas Commun.*, 31(9), 2013; pp. 47-65.
- [17] Jia X, Chen H, and Qi F. Technical models and key technologies of e-health monitoring. In *Proc. IEEE Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, 2012; pp. 23-26.
- [18] Sebestyen G, Hangan A, Oniga S and Gal Z. eHealth solutions in the context of Internet of Things. In *Proc. IEEE Int. Conf. Autom., Quality Test., Robot.*, 2014; pp. 1-6.
- [19] Caron X, Bosua R, Maynard SB, Ahmad A. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, 32 (1), 2016; pp. 4–15.
- [20] Sicari S, Rizzardi A, Grieco LA, Coen-Portisini A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, Vol. 76, 2015; pp. 146-164.
- [21] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2013; pp. 2266–2279.
- [22] Moosavi SR, Gia TN, Rahmani AM, Nigussie E, Virtanen S, Isoaho J, and Tenhunen H. SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. *Procedia Computer Science*, Vol. 52, 2015; pp. 452-459.
- [23] Abdmeziem MR and Tandjaoui D. An end-to-end secure key management protocol for e-health applications. *Computers & Electrical Engineering*, Vol. 44, 2015; pp. 184–197.
- [24] Ünalır MO, Can Ö, Sezer E. Ontoloji Tabanlı Bilgi Sistemlerinde Erişim Denetimi: Ulusal Aş1 Bilgi Sistemi İçin Durum Çalışması. *TUBAV Bilim Dergisi*, 3(3), 2010; s. 238-249.
- [25] Gruber T. Toward principles for the design of ontologies used for knowledge sharing. Technical Report KSL93-04, Knowledge Systems Laboratory, Stanford University, 1993.
- [26] Uschold M. Knowledge level modelling: Concepts and terminology. *Knowledge Engineering Review*, 13(1), 1998; pp. 5–29.
- [27] Sofia2. SOFIA2 IoT Platform: Technical View. [http://sofia2.com/docs/SOFIA2%20-%20Technical%20-%20IoT%20Platform%20\(oct%202014\).pdf](http://sofia2.com/docs/SOFIA2%20-%20Technical%20-%20IoT%20Platform%20(oct%202014).pdf), Son Erişim: Ağustos 2016.