

AKILLI ŞEHİRLERDE DAĞITIK VERİ İŞLEME

Yrd. Doç. Dr. Hüseyin BAYRAKTAR¹, Buket GÜLŞEN², Dursun Yıldırım BAYAR³, Bestami KARA⁴

¹ Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, huseyin.bayraktar@csb.gov.tr

² Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, buket.gulsen@csb.gov.tr

³ Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, dyildirim.bayar@csb.gov.tr

⁴ Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, bestami.kara@csb.gov.tr

ÖZET

Akıllı ve bağlı cihazların yaygınlaşması ve buna paralel olarak yaşanan teknolojik gelişmeler; yaşam kalitesini yükseltmeyi, ekonomik büyüme sağlamayı ve verimli kaynak dağıtımını amaçlayan akıllı şehirler ile ilgili yapılan araştırmalara hız kazandırmıştır. Bir akıllı şehir ağı, hâlihazırda bulunan bağımsız heterojen ağlar ve onların altyapıları arasındaki bağlantılar olarak tanımlanabilir. Akıllı şehirlerdeki heterojen yapı, veri kaynaklarının çeşitliliğinden ve bu verilerin; sensörler, kızılötesi kameralar gibi farklı cihazlar ve teknolojiler yardımıyla birçok kaynaktan toplanması sonucu elde edilen verilerin; format, büyüklük ve varış zamanı gibi farklı özelliklere sahip olmasından kaynaklanmaktadır. Cihazlarda, iletişim teknolojilerinde, ağ protokollerinde ve platformlarda bulunan mevcut heterojenlik göz önüne alındığında ağların birlikte çalışılabilirliği dikkatle üzerinde durulması gereken bir zorluk haline gelmektedir.

Anahtar Sözcükler: Akıllı şehirler, dağıtık veri işleme

ABSTRACT

DISTRIBUTED DATA PROCESSING IN SMART CITIES

The proliferation of smart and connected devices and parallel technological developments; It has accelerated the researches on smart cities, which aim to increase the quality of life, provide economic growth and efficient resource distribution. A smart city network can be defined as the links between existing independent and heterogeneous networks and their infrastructures. The heterogeneous structure in smart cities is due to the diversity of data sources and this data; The data obtained as a result of collecting from many sources with the help of different devices and technologies such as sensors, infrared cameras; This is due to the fact that it has different characteristics such as format, size and arrival time. Given the current heterogeneity in devices, communication technologies, network protocols, and platforms, the interoperability of networks becomes a challenge that needs careful attention.

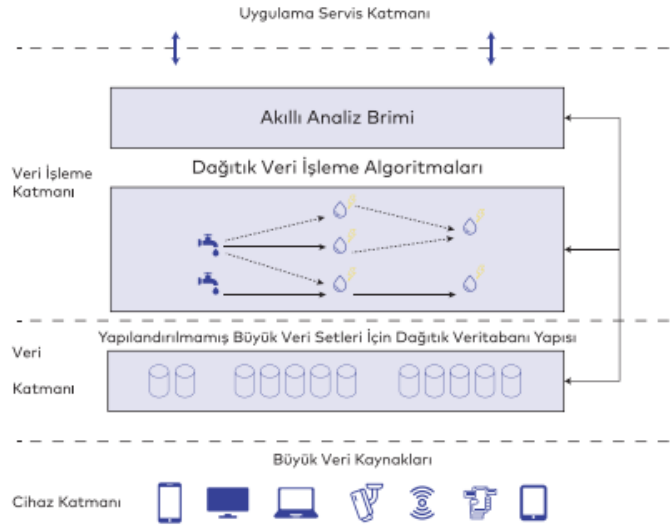
Keywords: smart cities, distributed data processing

1. GİRİŞ

Akıllı ve bağlı cihazların yaygınlaşması ve buna paralel olarak yaşanan teknolojik gelişmeler; yaşam kalitesini yükseltmeyi, ekonomik büyüme sağlamayı ve verimli kaynak dağıtımını amaçlayan akıllı şehirler ile ilgili yapılan araştırmalara hız kazandırmıştır. Bir akıllı şehir ağı, hâlihazırda bulunan bağımsız heterojen ağlar ve onların altyapıları arasındaki bağlantılar olarak tanımlanabilir. Akıllı şehirlerdeki heterojen yapı, veri kaynaklarının çeşitliliğinden ve bu verilerin; sensörler, kızılötesi kameralar gibi farklı cihazlar ve teknolojiler yardımıyla birçok kaynaktan toplanması sonucu elde edilen verilerin; format, büyüklük ve varış zamanı gibi farklı özelliklere sahip olmasından kaynaklanmaktadır. Cihazlarda, iletişim teknolojilerinde, ağ protokollerinde ve platformlarda bulunan mevcut heterojenlik göz önüne alındığında ağların birlikte çalışılabilirliği dikkatle üzerinde durulması gereken bir zorluk haline gelmektedir.

Yaklaşık 10 yıl önce yapılan çalışmalarda odak noktası, radyo frekansı tanımlama (Radio Frequency Identification-RFID) etiketlerine dayanarak nesnelerin izlenebilmesi ve takip edilebilmesiydi (Bawany vd., 2015:1). Nesnelerin interneti (IoT), eşsiz bir şekilde adreslenmiş birbirine bağlı nesnelerin dünya genelinde oluşturduğu ağ şeklinde tanımlanmaktaydı. İlerleyen süreçte, heterojen nesnelerin sayısındaki inanılmaz artış ile yapılan araştırmalar, semantik ve servis odaklı perspektiften nesnelerin beraber çalışılabilirliği, sunumu ve soyutlanması konularına kaymaya başlamıştır (Atzori vd., 2010:2787). IoT uygulamalarını “akıllı” yapan özellik büyük veridir. Bu veri merkezli görüş, akıllı uygulamalar yaratırken en değerli şey olarak tanımlanmaktadır. IoT verisinin boyutu arttıkça, işlenmemiş veriyi transfer etme ve merkezi bir veri ortamında işleme imkansız hale gelmeye başlar. Özellikle düşük kalitedeki verinin, veri merkezine transfer edilmesinin ardından; verinin sadeleştirilmesi, birleştirilmesi ve soyutlama gibi ek işlemlere ihtiyaç duyulmaktadır. Ön işlem süreci zaman isteyen masraflı bir süreçtir. Genellikle servisin sağlanmasında yüksek gecikme sürelerine sebep olmaktadır. Bu nedenle büyük verinin en temel bileşenlerinden biri olduğu akıllı şehir sistemlerinde, merkezi bir veri işleme mimarisi yerine; etkili bir dağıtık veri işleme mimarisi kullanılması daha etkin sonuçlar verecektir. Böylece sistem üzerinden birbirine bağlı olan akıllı cihazlar, veri tabanları ve diğer veri işleme

birimlerinin işlem kapasitelerini birleştirerek, verinin analizini ve işlenmesini daha kısa sürede gerçekleştirebilecektir. Şekil 1’de akıllı şehir uygulamalarının genel mimarisi ile dağıtık veri toplama ve işleme katmanları görülmektedir



Şekil 1. Akıllı Şehir Mimarisi ve Dağıtık Veri Toplama/İşleme Katmanları

Veri işleme mimarisi, akıllı şehir uygulamalarında belirgin bir rol oynamaktadır. Etkif bir veri altyapısının uygun, paralel ve dağıtık veri işleme mimarileri ile kullanılması günümüz akıllı şehir servislerini bir sonraki aşamaya taşıyacak güce ve kapasiteye sahiptir. Veri işleme platformunda yapılacak bu kuvvetlendirme ile uygulama alanına yenilik ve yarar getirilmesinin yanında akıllı şehir vizyonunun bir bütün olarak geliştirilmesi de mümkün hale gelecektir.

2. DAĞITIK VERİ İŞLEME MİMARİSİ

Bir akıllı şehir inşa etmenin önündeki zorluk; cihazlar, ağ protokolleri, kurallar ve platformlar açısından çeşitliliğe, bir diğer deyişle heterojenliğe sahip olan farklı türdeki ağların birbirine bağlanması olacaktır (Tourani vd., 2019:93).

Mevcut yaklaşımlar, ağda merkezi bir birim olarak, veri yönetim katmanı kullanmaktadırlar (Silva vd., 2018:697). Bu katmanda farklı kaynaklardan gelen veri toplanır, organize ve analiz edilir ve ardından depolanarak akıllı karar aşaması için hazırlanır. Böyle bir merkezi veri işleme mimarisinin sahip olduğu birçok olumsuzluk bulunmaktadır. Merkezi mimariler belirli ihtiyaçlara odaklanmaları ve esnek olmamaları nedeniyle değişen kullanıcı ihtiyaçlarına beklenen düzeyde cevap verememekte ve teknolojik gelişmelere uyum sağlayamamaktadır. Verinin merkezi bir noktada toplanması ve işlenmesi, aynı zamanda karar verme mekanizmasının tek olması, verinin ihtiyaç duyulsa bile lokal olarak kontrol edilememesi anlamına gelmektedir. Bu durum servis ihtiyaçlarına lokal bazda istenilen düzeyde cevap verilememesi demektir. Büyük miktardaki verinin bir merkezde toplanması, işlenmesi ve karar verme işlemlerinin gerçekleştirilmesi yüksek işletim maliyetine de sebep olmaktadır. Aynı zamanda olası bir arıza ya da siber saldırı durumunda tek merkezden yönetilen böylesi bir mimari her zaman bulut tabanlı sistemlere kıyasla veri kaybına daha açıktır. Sonuç olarak merkezi veri işleme yaklaşımı, oldukça yüksek veri seviyelerinde çalışan heterojen veri kaynakları, protokolleri ve sistemleriyle ilgilenmek için genellikle yavaş ve verimsiz kalmaktadır.

Merkezi yaklaşımın yukarıda bahsedilen olumsuzluklarını ortadan kaldırmak için geliştirilen yaklaşımlar, çoğunlukla ağdaki karar verme işlemlerini tamamen dağıtık bir biçimde gerçekleştirmektedir.

2.1. Adlandırılmış Veri Ağ Haberleşmesi

Bilgi merkezli ağ haberleşmesi (The Informatic-Centric Networking - ICN), “sunucu-merkezli” mevcut iletişim modelini, verinin ana nitelik olduğu “veri-merkezli” bir yaklaşıma taşımıştır. Adlandırılmış ağ haberleşmesi (Named-Data Networking-NDN), en yaygın kullanılan bilgi merkezli ağ haberleşmesi çeşididir. Veri kaynak/ hedeflerini tanımlamak için IP adreslerini kullanan, IP ağlarının aksine; NDN mimarisinde ana fikir ise eşsiz içeriğin adlandırılması, yaygın ön belleğe alma ve adlandırma tabanlı yönlendirmedir (Named Data Networking, 2020) (Jacobson vd., 2009:1) (Zhang vd., 2014:66). NDN doğal bir akış kontrolüne sahip toplama tabanlı bir iletişim mimarisidir. Her bir NDN istek paketi, bir parça verinin ortaya çıkmasına sebep olur. Bu veri merkezli yaklaşım, IoT uygulamalarının kendine özgü üretici/tüketici tabiatı ile ağ operasyonlarını düzenler. Bu durum da veri merkezli yaklaşımın IoT ağları için mükemmel uygunlukta olduğunu göstermektedir.

NDN’de yönlendiriciler; gelen istek tablosu, yönlendirilen bilgi bazı ve içerik deposu ile donatılmışlardır. Yönlendirilen bilgi bazı, IP yönlendiricilerdeki yönlendirme tablosuna benzer yapıda ve bir yönlendirme algoritması kullanılarak oluşturulur. Bir istek paketini alan her düğüm; kendi içerik deposunu, içerik adı ile kontrol eder. Eğer içerik mevcut değil ise yönlendirici gelen istek tablosuna bakarak talep edilen içerikle ilgili bir kayıt olup olmadığını kontrol eder. Eğer bu kontrol başarılı sonuçlanırsa, yönlendirici gelen isteğin ara yüzünü, gelen istek tablosundaki kayda ekler ve isteği düşürür. Aksi takdirde yönlendirici yeni gelen istek tablosu kaydı oluşturarak bu kaydı iletilen bilgi bazını kullanıp hedefine doğru yönlendirir.

Bir istek, ilgili içeriği önbelleğinde saklayan ara bir yönlendirici tarafından ya da içerik sağlayıcı tarafından karşılanabilir. İki durumda da içerik, istekte bulunana gönderilmek üzere aynı yolu takip edecek şekilde iletilir. Yönlendirici bir içerik yığını aldığında ilgili isteği aldığı ara yüzler boyunca iletir. Yönlendirici aynı zamanda içeriğin bir kopyasını sonradan gelen istekler için kendi içerik deposunda saklar. NDN’in en önemli bölümü, strateji katmanının bir düğüm katmanları arası bilgiyi kullanarak detaylı ve akıllı yönlendirme kararlarını verebilmesi için izin vermesidir. NDN protokolünün temel tasarım prensipleri aşağıdaki gibi sıralanabilir (Named Data Networking, 2020):

- Evrensellik: NDN tüm uygulamalar ve ağ ortamları için ortak bir ağ protokolü olmalıdır.
- Veri merkezliliği ve Değişmezliği: NDN eşsiz bir şekilde adlandırılmış, değişmez veri ve istek paketlerini kullanarak yakalamalıdır.
- Veriyi Doğrudan Güvene Alma: Güvenlik veri paketlerinin özelliği olmalıdır. Paketin hareket halinde olması ya da durması bunu değiştirmemelidir.
- Hiyerarşik İsimlendirme: Paketler hiyerarşik isimleri taşıyarak çoğullamadan çıkarma ve yapılandırılmış içeriği sağlamalıdır.
- Ağ İçi İsim Keşfi: İstekler, veri paketlerine erişmek için tamamlanmamış isimleri de kullanabiliyor olmalıdırlar.
- Adım Adım Akış Dengeleme: Her link üzerinden istek paketleri sadece bir veri paketini geri getirebilmelidir.

2.2. Bilgi Merkezli ve Servis Tabanlı Mimari

Son dönemde birkaç farklı çalışmada NDN geliştirilerek akıllı şehirler için kullanılmıştır. Bu yaklaşımlar akıllı şehirlerde iletişim (Bouk vd., 2017:105), NDN platformunda akıllı servislerin tasarımı-yönetilmesi (Piro vd., 2014:169) ve bir akıllı şehir ağındaki cihazların geniş ölçekli kurulumu için güvenli yönlendirme (Mick vd., 2017:755) konularına odaklanılmışlardır. Ancak bu çalışmalarda mevcut heterojen ve kendini yöneten ağların bütüncül bir şekilde nasıl entegre edileceği sorununa cevap bulunamamıştır.

Bu sorundan yola çıkılarak yapılan araştırmalar sonucunda NDN’in geliştirilerek, ağ içi verinin paylaşımının ve kaynak hesaplamasının kusursuz ve verimli bir şekilde yapılabileceği ortaya konmuştur (Tourani vd., 2019:93). NDN veri adlandırma, yayılmış ön belleğe alma, ağ içi işleme ve güvenlik özellikleri kapsamında akıllı şehir ağlarının ihtiyaçlarının etkili bir şekilde belirlenebilmesi için kullanılabilir. NDN kaynakları isimler kullanılarak paylaşılmasına imkân verir. Böylelikle IoT cihazlarının birbiriyle bağlantılı otonom ağlarının kurulmasının kolay bir şekilde yapılmasına olanak sağlar.

Bilgi merkezli akıllı şehir (iSmart) mimarisi ile NDN kullanılarak tüm akıllı şehir katılımcıları için veri ve servis merkezli bir sistem tasarımı gerçekleştirilmiştir (Tourani vd., 2019:93). Bu mimari ile bağımsız bir şekilde kendilerini yönetebilen IoT/Siber Fiziksel Sistem ağlarından oluşan bir akıllı şehir sistemi tasarlamak mümkündür. Bu tipteki ağların bulutta ya da kendi özel sunucuları üzerinde çalışan servisleri, aynı akıllı şebekelerde olduğu gibi birbirinden bağımsız olarak işleyecektir. Bir başka deyişle, IoT cihazlarının algılayıcı verileri iletmek ve emir/kontrol mesajlarını almak üzere bir sunucu ile iletişim halinde olacakları servis tabanlı bir mimari tasarlanmıştır.

2.3. Sınır Tabanlı Veri ve Hesaplama Paylaşımı

Sınır bilişim çoğunlukla merkezi kontrol ve komuta birimlerine dayalı çalışır. Bu birimler ağdaki istatistiki bilgileri toplar, yükleri hesaplar, karar verme, yük dengeleme ve servis izleme işlemlerini gerçekleştirir. Ancak böylesi bir merkezi tasarım esnek değildir ve sistemi hatalara açık hale getirir.

Geleneksel IP mimarilerinde; içerik, lokasyon ve durum mesajlarının fiziksel IP cihazlarında depolanması ve haritalanması gerekmektedir. Bu karmaşık haritalama işlemi; gecikmeye, kaynakların verimsiz bir biçimde kullanımına ve hata oranında artışlara sebep olur. Tüm bunlar zaman konusunda hassas uygulamaları içinde barındıran akıllı şehir senaryoları için çok vahim sonuçlar doğurabilir. NDN’de istek ve veri paketleri, içeriği kolayca tanımlayabilecek ve yönlendirme, güvenlik, uygulama ihtiyaçlarını haritalamaya ihtiyaç kalmaksızın gerçekleştirebilecek anlamsal adlandırmayı kullanırlar. İçerik hakkında bilgi sahibi olan böyle bir adlandırma mekanizması çoklu alanlar üzerinden farklı paydaşlar arasında veri paylaşımını ve iş birliğini mümkün kılar.

Akıllı şehirlerde sınırda verinin toplanması, iletişim ve görevlerin icra edilmesi, ağda sıkışmalara ve hesaplama düğümlerine aşırı yük binmesine sebep olur. Sıklıkla bu gibi hesaplama hassasiyeti olan ortamlarda uç kullanıcılar benzer görevlerin gerçekleştirilmesini talep ederler. Fakat sınır bilişimin kurulumundan kaynaklı mevcut hesaplama

sonuçlarının tekrar kullanılmasından ziyade, hesaplamalar tekrar yapılır. Bu da işlem gücünün lüzumsuz yere kullanılması anlamına gelmektedir. Mevcut IP tabanlı sistemlerde hesaplamaların yeniden kullanılması, görev benzerliğini tanımlamak için kullanılan metaveri sadece uygulama katmanında kullanılabilir olduğundan zor olabilir. NDN’de içerik bilinçli adlandırma hesaplamasının yeniden kullanılmasına yardımcı olarak gereksiz hesaplamaların yapılmasının önüne geçebilir. Sınır bilişim düğümleri isim filtrelemesini kullanarak ve içeriği sınıflandırarak önceden yapılmış hesaplamalar arasından yapılan aramayı hızlandırabilir.

3. TASARIMDA KARŞILAŞILABİLECEK ZORLUKLAR

3.1. Gizlilik

NDN’in içerik adlandırma ve yaygın önbelleğe alma özellikleri veri paylaşımına olanak tanımaktadır. Ancak bu şekilde bir veri paylaşımı gizliliğin ihlal edilmesine sebep olabilir. NDN’in avantajlarından yararlanabilmek için ek gizlilik mekanizmalarına ihtiyaç duyulmaktadır.

Akıllı şehir uygulamalarının çokluğu ve karmaşık yapısı, kullanılan farklı teknolojiler ve saldırganlar, vatandaşların karşılaşılabileceği olası gizlilik risklerinin tespitini ve takibini zorlaştırmaktadır. Çoğunlukla bu riskler uygulamalardan kaynaklanmayıp uygulamaların altyapılarındaki teknolojiyi kullanma şekillerinden kaynaklanır. Örneğin toplu taşımada kullanılan akıllı kartlar tek başlarına bir gizlilik riski yaratmamalarına rağmen üzerlerinde taşınan bilginin; kişinin adı-soyadı, yaşı, özür durumu ve gün içerisinde kullandığı rota gibi kişisel bilgiler olması bu akıllı kartın gizlilikle ilgili olası bir problem kaynağı haline gelmesine neden olur. Bu nedenle uygulamaların yanı sıra uygulamanın altyapısında kullanılan teknolojinin ve toplanan verinin gizlilik problemi yaratıp yaratmadığı iyi bir şekilde analiz edilmelidir.

Dağıtık veri işlemenin gerçekleştirildiği akıllı şehir uygulamalarında gizlilik birçok açıdan ele alınabilir. Örneğin iletişim kanalları üzerindeki gizliliğin korunumu bazı durumlarda zor olabilir. Havaalanları gibi kamuya açık alanlarda yer alan ağ trafiğinin her zaman şifrelenmesi gerekmediğinden veriler; erişim noktaları, ara düğümler ve diğer kişiler tarafından izlenebilir. Bu veri sızıntısı, kablosuz iletişimin şifrelenmesi ve tüm web servislerinin ve mobil uygulamaların SSL/TLS ile güvence altına alınması sayesinde önlenemez. SSL/ TLS kullanımı yaygın olsa da protokolün yanlış kullanımı gizlilik sızıntılarına sebep olabileceğinden bu durum istatistikî analiz araçlarının kullanımı ile tespit edilebilir ve doğrulama işlemi dinamik kütüphanelerle gerçekleştirilebilir.

Her ne kadar kamuya açık internet imzasız bir şekilde kullanılsa da statik MAC adreslerini ya da sistem parametrelerini kullanan parmak izi kontrolü teknikleri kullanıcıların takip edilmesini ve yeniden kimliklendirilmesini sağlar. Akıllı şehir sistemlerinin temel bileşenlerinden biri olan mobil cihazların kullanımı da gizlilik sorunlarını beraberinde getirmektedir. Modern mobil cihazlar kullanıcıların çeşitli hareketlerini takip etmeye yarayan çok sayıda sensör ile donatılmıştır. Ayrıca bu cihazlar, farklı üreticiler tarafından, farklı hedeflere hizmet edecek şekilde çeşitli bileşenlerle donatıldıklarından kullanıcıların hassas verisinin korunması daha da zor hale getirmektedir. Mevcut gizlilik çözümleri daha küçük ölçekteki mobil cihaz ekosistemlerini hedef aldıkları için yetersiz kalmakta ve kullanıcıları savunmasız bırakmaktadır. Ayrıca mobil cihazlar üzerinde çalışan üçüncü parti uygulamaların gereğinden fazla erişim iznine ihtiyaç duymaları ve kullanıcıların da çoğunlukla bu isteği onaylamaları da gizliliği tehlikeye düşürmektedir. Üreticiler tarafından bu isteklere sınır getirilmesi ya da kullanıcıların bilinçlendirilmesi alınabilecek önlemlerden bazılarıdır.

Akıllı kartların kullanımı sırasında ortaya çıkabilecek ana gizlilik problemi kartla yapılan işlemlerin hassas veri barındırmasından kaynaklanmaktadır. Kart sahibi ile ilgili konum ve rutin gibi hassas bilgiler farklı kullanıcıların verileri arasında ilişkilendirilme yapıldığında ortaya çıkabilir. Akıllı kartlar vasıtasıyla toplanan veriler, kullanıcıya servis sağlamanın yanı sıra profil tespiti ve takip amacıyla da kullanılabilir. Bunun önüne geçmek için kimlik doğrulaması ve servisin birbirinden ayrı tutulması gerekmektedir. Kullanıcı kimliğini açığa çıkarmadan, sunulacak hizmete erişim hakkı olup olmadığına kriptografik yaklaşımlar ve kimlik dışı veri alanları kullanılarak karar verilmesi mümkündür. Servis ve kimlik doğrulamanın ayrışması gizliliğin sağlanmasını tam olarak garanti etmemektedir. Çünkü servis verisi çoğunlukla kimliğin yeniden tespiti için yeterli olabilmektedir. Bunu önlemek için de toplanan ve depolanan verinin miktarı azaltılabilir. Örneğin akıllı kartların eşsiz kimliği izlenebilir ve yeniden kimlik tespiti için kullanılabilir. Bu nedenle bu verinin kaydedilmemesi gerekmektedir. Ücretlendirmeyi doğru şekilde yapabilmek için tam konum yerine ulaşım bölgelerinin kullanılması, uç bölge sunucularıyla bağlantı zorunluluğunu ortadan kaldıracak için her bir kullanıcı ile ilgili toplanacak olan verinin minimize edilmesini sağlar.

Geleneksel mimarilerde veri açık bir şekilde yayınlanmaktadır. Ancak akıllı şehirlerde toplanan büyük miktardaki veri olduğu gibi paylaşılmalıdır. Tüm kişisel bilgilerin basit bir şekilde veriden çıkarılması da yeniden tanımlamanın önüne geçmek için bir çözüm değildir. Örneğin Amerika Birleşik Devletleri’nde nüfusunun %87’lik kısmı sadece posta kodu, doğum tarihi ve cinsiyet bilgilerine dayanarak tespit edilebilmektedir. Verinin birleştirilmesi gizlilik problemlerini azaltabilir. Veri servisi sağlayıcısından bile saklanıyorsa o zaman birleştirme işlemi benzer yapıya şifrelemeye dayanan kriptografik protokollerin kullanılması sayesinde en etkili yöntem haline gelebilir. Verinin gizlenmesi de başka bir çözüm olarak sunulabilir. Anonimleştirme yöntemleri sayesinde veri anlamını korurken aynı

zamanda kişisel ve hassas verinin tespiti zor hale getirilmektedir. k-anonimleştirme gibi yöntemler bu amaçla sıklıkla kullanılmaktadır.

3.2. Güvenlik

Güvenlik ve gizlilik birbirleriyle yakın ilişki içindedirler. Güvenlik olmadan etkili bir gizlilik koruması düşünülemez. Örneğin kamuya açık alanda kayıt yapan ve kaydettiği görüntüleri başka bir yere ileten bir kamera, yalnızca gizlilik probleminde yol açarken aynı kameranın sunucu ile iletişimde yaşanan herhangi bir güvenlik problemi aynı zamanda gizlilik probleminin de ortaya çıkmasına neden olabilir. Bu nedenle güvenlik koruması olmadan gizliliğin tamamen korunduğundan bahsedilemez. IoT cihazlarının yaygınlaşması ve adaptasyonu, yeni güvenlik tehditleri ve saldırıları için zemin hazırlamaktadır. Akıllı şehirler açısından siber saldırılar yıkıcı sonuçlar doğurabilir. Örneğin saldırganlar ağa sızarak şehir genelinde elektrik kesintisine sebep olabilir. Bu nedenle akıllı şehir uygulamalarında güvenlik tedbirlerinin alınması çok önemlidir.

Akıllı şehirlerin bileşenlerinin birbirinden bağımsız yapıları da güvenlik problemlerini kaçınılmaz kılmaktadır. Akıllı cihazlardaki algılayıcı ara yüzler güvenlik sorunlarına sebep olabilmektedir. Siber fiziksel sistemlerin algılayıcı kanalları kötüçül yazılımlar yoluyla ile cihazları etkilemek için kullanılabilir. Benzer güvenlik saldırıları; akıllı otonom cihazların etki altına alınarak uzun ya da kısa vadede sürüş kararlarının dış müdahalelere maruz kalmasına yol açabilir. Erişim kontrolünün kısıtlanması, kayıtlı haldeki veriye erişimin hem yetkilendirilmiş hem de yetkilendirilmemiş kişilere karşı koruma altına alınmasını sağlamaktadır. Erişim kontrolü bir gerekliliktir ve aynı zamanda yetkilendirilmiş kişilerin erişim haklarını haksız şekilde ve kötüye kullanmasına engel olduğu için güvenlik açısından oldukça faydalıdır. Bilgi akışı bir sistem üzerinden takip edilebilir ve veri sahibinin erişim politikasına uyulması zorunlu tutulabilir.

Erişim kontrolü özellikle otonom sistemler açısından önemlidir. Çünkü bu sistemlere internet üzerinden erişim sağlanabilir ve uzaktan kontrol edilebilir. Akıllı ev aletlerinin uzaktan kontrolü gibi görece daha zararsız saldırılardan otonom araçlara müdahale edilmesi gibi ölümcül sonuçlar doğurabilecek senaryolara kadar birçok güvenlik açığı erişim kontrolünün yetersiz olmasından kaynaklanmaktadır.

Kriptografik protokoller çoğunlukla güvenlik problemlerini ortadan kaldırmak amacıyla kullanılsalar da bu protokollerin yanlış şekilde tasarımı da güvenlik sorunlarına sebep olabilmektedir. Eğer bir sistem için tasarlanmış güvenlik protokolüne üçüncü şahıslar tarafından erişim sağlanırsa; bu aynı zamanda gizliliğin de tehlike altına girmesi anlamına gelmektedir. Bu riski ortadan kaldırmak için güvenlik algoritmalarının ve sistemi koruyan güvenlik bileşenlerinin dikkatli bir şekilde tasarlanması gerekmektedir.

Zamanlama ve enerji tüketimini kontrol eden yan kanallar, bilgi kriptografik olarak korunsalar bile bilgi sızıntısına sebep olabilmektedir. Akıllı sayaçların, IoT cihazlarının ya da akıllı cihazların üzerindeki bilgilere erişilmesi yan kanalların kullanımı ile mümkün hale gelmektedir. Akıllı cihazlar üzerindeki sensörler yardımıyla özellikle konum bilgisine ulaşılabilmektedir. Giyilebilir cihazlar için en büyük güvenlik problemlerinden biri cihaz üzerinden gereğinden fazla bilginin üçüncü şahıslara aktarılmasıdır. Bu bilgiler kullanılarak başka güvenlik saldırılarına zemin oluşturulabilir. Bu cihazlar üzerindeki sensörler ve iletişim kanallarının korunması da bilginin korunabilmesi ve dolayısıyla güvenliğin sağlanabilmesi açısından önemlidir. IoT cihazlar arasında büyük miktarda verinin paylaşılıyor olması güvenlik açısından sorunlar yaratabilmektedir. Tek bir cihazdaki güvenlik zafiyeti tüm sistemin tehlikeye düşmesine sebep olabileceğinden veri aktarımının güvenli kanallar üzerinden ve şifrelenerek yapılması gerekmektedir.

Blok zinciri teknolojisi de akıllı cihazlarda güvenliğin sağlanması için sıklıkla kullanılmaktadır. Blok zincirleri işlemleri kaydeden, depolayan ve kamuya açık şekilde doğrulanabilecek değişmez kayıt defterleridir. Yeni işlemler bloklar halinde toplanır ve kriptografik bir bulmaca çözülerek kayıt defterine kaydedilir. Her yeni blok kendinden bir öncekine bağlıdır için bu yapıya blok zinciri adı verilmektedir.

Blok zincirlerinde kullanıcılar takma isim kullanabilirler. Çünkü sadece kamuya açık anahtarları ile ilişkilendirilmektedirler. Blokların işlenmesi ile dağıtık bir uzlaşma sağlanabildiği için güvenilir üçüncü şahıslara ya da kurumlara ihtiyaç duyulmamaktadır. Kripto para işlemleri için tasarlanmış olan blok zinciri sistemi aynı zamanda finansal olmayan uygulamalar için de kullanılabilir. Özellikle IoT uygulamalarında güvenlik ve gizliliğin sağlanması açısından faydaları bilimsel çalışmalar yoluyla ortaya konulduğundan akıllı şehir uygulamalarında da sıklıkla kullanılmaktadırlar. Blok zincirlerinin kullanılması, kullanıcıların kendi verilerinin sahibi olmasına ve kontrol edebilmelerine olanak tanıyan dağıtık sistemlerde oldukça kullanışlı bir yaklaşımdır.

3.3. Düzenleme

Akıllı şehirler uluslararası sistemlerde veri değış tokuşunu yönetebilirler. Farklı bölgeler ya da ülkeler diğer bölge ya da ülkelerle koordinasyonunu sağlamak için kendi yasalarını ve stratejilerini geliştirebilirler. Bunların yanı sıra düzenleme ve standartlaştırma her bir paydaşın sorumluluklarını tanımlamada, olası çatışma durumlarında ve üretilen verinin sahipliği konusundaki tartışmalarda çözüm oluşturabilir. Düzenleme işleminin karakteristiği yönetmelikler ve kanuni yaptırımlarla akıllı şehir servislerine uyumlu olacak şekilde belirlenmektedir. Avrupa Birliği ülkelerinde

hâlihazırda tanımlanmış düzenlemeye ilişkin kurallar bulunmaktadır. Bu kurallara tüm ülkelerce uyulması zorunlu kılınmıştır. Akıllı şehir servislerinin mevzuat tarafından belirlenen temel özellikleri şu şekilde sıralanabilir:

- Bazı ülkelerde ulusal kanunlar veri trafiğinin kesintiye uğramasını gerektirebilir.
- Kabul edilenden daha sık gelişen servis hatalarından kaçınılabılır.
- Vatandaşların kişisel bilgilerinin korunması bir hak ve zorunluluktur.
- Cihazlarda ya da servis seviyesinde gerçekleşen siber saldırılardan kaçınmak ve önlemek için gerekli güvenlik mekanizmaları sağlanmalıdır.
- Veriye ve servislere açık erişimin mümkün olması ve bunlar arasında birlikte çalışabilirliğin bulunması gerekmektedir.

Tüm bu ihtiyaçların farklı ülkelerde aynı şekilde sağlanabilmesi her zaman mümkün olmayabilir. Ülkelerin iç dinamikleri, teknik altyapıları ya da ulusal kanunlar bu gereksinimlerden biri ya da birkaçını gerçekleştirmeye engel olabilir. Bu gibi durumlarda verinin akıllı cihazlar ve sistemler arasında paylaşılması esasına dayanan dağıtık veri işleme sisteminde aksaklıklar ve problemler baş gösterecektir. Bu ve benzeri sorunların ortadan kalkabilmesi için bölgesel ve küresel çapta kurulların oluşturulması ve ortak kararlar alınarak veri işleme, veri paylaşımı, gizlilik ve güvenlik gibi konularda tüm ülkelerin ortak paydada buluşmasını sağlayacak yeni düzenlemeler yapılması sürece katkı sağlayabilir.

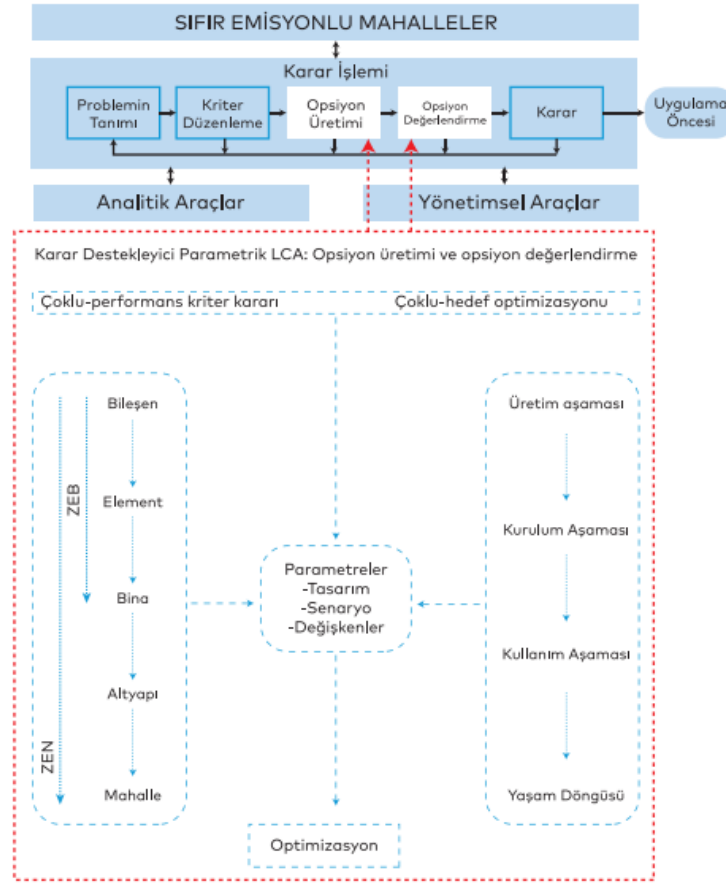
4. UYGULAMALAR

Günümüzde kentsel alanlara yerleşen ve buralarda yaşamaya başlayan insan sayısı oldukça fazladır. Bu popülasyon her geçen gün artmaktadır. Bu durum beraberinde altyapıda ve servislerde bir yoğunluk yaşanmasına sebep olmaktadır. Birleşmiş Milletler'in raporuna göre bu yüzyılın ortasıyla beraber dünya nüfusunun %68'ini şehirlerde yaşayan insan popülasyonu oluşturacaktır. Bu hızlı artış sonucunda şehirlerde yaşayanlara enerji, su ve diğer temel servislerin verimli ve etkili bir şekilde sağlanması problem olmaya başlamaktadır. IoT teknolojisinin altyapı olarak kullanıldığı ve farklı ağ teknolojileri ile şehirlerin daha akıllı hale getirilmesini amaçlayan akıllı şehir sistemlerine yönelik çalışmalar yoğun bir şekilde dünya genelinde devam etmektedir. Akıllı şehir mimarilerinin en temel özelliklerinden biri de kullanıcı profili, kullanılan cihaz, iletişim teknolojileri ve ağ protokollerindeki çeşitlilik yani heterojenliktir. Bu heterojen yapı beraberinde işlenmeyi ve analiz edilmeyi bekleyen büyük miktardaki veriyi de getirmektedir. Bu ölçekte ve sürekli bir akışa sahip olan verinin merkezi bir noktadan kontrol edilmesi ve yönetilmesi neredeyse imkânsızdır. Bu nedenle modern akıllı şehir mimarilerinde merkezi yaklaşım yerine işlem gücünün paylaşılması esasına dayanan, servis ihtiyaçlarının lokal ve sistem bazında daha hızlı karşılanmasına olanak veren dağıtık veri işleme mimarileri esas alınmaya başlamıştır.

Dağıtık veri işleme mimarilerindeki sis, bulut ve sınır bilişimden oluşan çok katmanlı yapı işlemlerin dağıtılarak sistem performansının olabilecek en ileri noktaya taşınmasına yardımcı olur. Dünya üzerinde akıllı şehir uygulamalarında dağıtık veri işleme modellerinin kullanıldığı birçok örnek bulunmaktadır.

4.1. Norveç

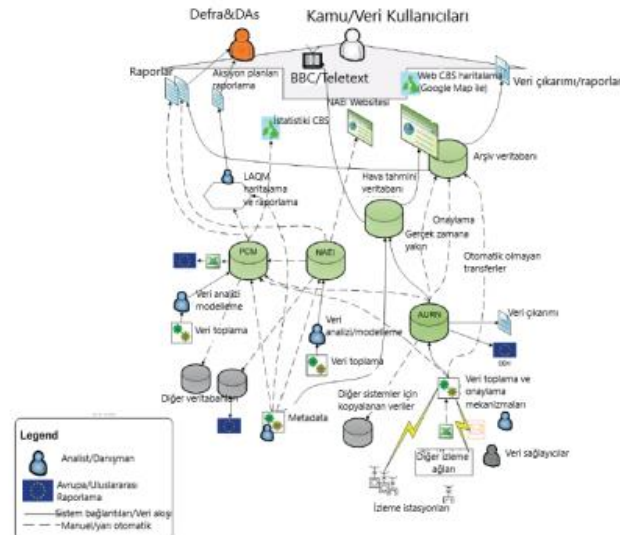
Norveç, Kuzey Avrupa'da akıllı şehir uygulamaları konusunda önder ülkelerden biridir. Birçok batı ülkesinde olduğu gibi binalar enerji tüketiminin en çok gerçekleştiği yapılar ve sera gazı emisyonunun neredeyse 1/3'lük kısmından sorumludurlar. Bu nedenle ülke genelinde şehirleri akıllı ve çevreye duyarlı hale getirmek için yapılan birçok çalışma bulunmaktadır. Bunlardan biri de Sıfır Emisyon Binalar (Zero Emission Buildings) projesidir. Bu proje kapsamında binalar tarafından üretilen verinin akışını ve yönetimini sağlayacak dağıtık bir veri işleme mimarisi tasarlanmıştır. 6 farklı şehirdeki 9 akıllı bina üzerine farklı kaynaklardan gelecek çeşitli tipteki verinin IoT cihazları ile toplanabilmesi için cihazlar yerleştirilmiştir. Tek bir binada veri işleme gerçekleştirmek yerine binaları bir grubun üyeleri haline getirerek bulut, sis ve sınır bilişimden oluşan çok katmanlı ve bilgi merkezli yapı ile IoT cihazlarla bulut arasındaki iletişim sağlanmakta ve elde edilen veri farklı kaynaklar tarafından dağıtık bir şekilde işlenmektedir. Bu da veri işleme sırasında ihtiyaç duyulan enerjinin farklı merkezlerden temin edilmesini sağlamakta ve işlem sonucunda ortaya çıkacak emisyonu düşürmektedir. Projeye ait mimari şeması Şekil 2'te gösterilmektedir.



Şekil 2: Sıfır Emisyonlu Binalar Projesi Mimarisi (From Zero Emission Buildings (ZEB) to Zero Emission Neighbourhoods (ZEN): A Mapping Review of Algorithm-Based LCA, Erişim Tarihi: 1 Mart 2021)

4.2. İngiltere

İngiltere özellikle hava kirliliğinin insan yaşamı üzerindeki olumsuz etkisini azaltmak adına akıllı şehir uygulamalarına öncelik vermektedir. Ülke, tarihi boyunca birçok kez yaşanan hava kirliliği sebebi ile ulusal ölçekte krizlerle başa çıkmak zorunda kalmıştır. Efektif bir şekilde hava kirlilik seviyesini ölçmek ve vatandaşların gündelik aktivitelerini daha iyi planlayabilmek ve olası problemleri önleyebilmek için kirlilik tahminlerinin yapılabilmesi amacıyla geliştirilen Londra Hava Kalitesi Ağı (London Air Quality Network) projesi hayata geçirilmiştir. Proje kapsamında farklı merkezlerden toplanan hava kalitesi verileri akıllı algoritmalar, dağıtık mimari ve dağıtık veri işleme platformları ile analiz edilmiştir. Proje sonuçları kullanılan dağıtık mimarinin başarısını ortaya koymaktadır. Şekil 3'da projeye ait iş-akış şeması görülmektedir.



Şekil 3: Londra Hava Kalitesi Ağı (Air Quality Data Management and Integration System Report, Erişim Tarihi: 1 Mart 2021)

4.3. Polonya

Akıllı şehir sistemlerinde verinin düzenli ve gerçek zamanlı yapısı nedeniyle, verinin elde edilmesi, taşınması ve analizinin verimli bir şekilde gerçekleştirilmesi çok önemlidir. Bu sayede kullanıcıya akıllı şehir servislerinin gerçek zamanlı ya da minimum gecikme ile sunulması mümkün olmaktadır. Polonya son yıllarda geliştirdiği akıllı şehir projeleri ile bu alanda kendini göstermeye başlamıştır. Varşova’da gerçekleştirilen ve VaVel akıllı şehir projesinin bir parçası olan uygulamada araç hareketlerinin analizi ve gecikme tahmini işlemleri Apache Flink dağıtık veri işleme platformu üzerinden yapılmaktadır. Bu sayede şehir içi trafik durumu ile ilgili kullanıcılar gerçek zamanlı bilgilendirilmekte ve olası gecikmelerin önüne geçilmektedir.

4.4. Çin

Dünyanın en kalabalık popülasyonlarından birine sahip olan Çin akıllı şehir uygulamalarının insan yaşamına olumlu etkilerinin ve yönetsel avantajlarının farkında olan ve uzun süredir birçok farklı akıllı şehir uygulamasını ve projesini hayata geçiren ülkelerden biridir. Hangzhou metropolü 7 milyondan fazla nüfusu ile Çin’in en kalabalık 5. şehri unvanını elinde tutmaktadır. Böylesi büyük bir insan nüfusunu ve onlar için geliştirilen servisleri yönetmek için geliştirilen City Brain projesi ile Hangzhou genelinde farklı kaynaklardan gelen veriler toplanmaktadır. Toplanan verinin analiz edilmesi amacıyla proje üzerinde geliştirilen dağıtık veri işleme mimarisi için Apache Flink mimarisi kullanılmakta bu da verinin hızlı ve etkili bir şekilde analizine olanak vermektedir.

2. SONUÇLAR

Teknik gelişmelere ek olarak akıllı ve bağlı cihazların sayısı ve kullanımındaki hızlı artış, akıllı şehir sistemlerinin tasarlanmasına ve hayata geçirilmesine önayak olarak şehir hayatının kalitesini arttırmaya, ekonomik büyümeye ve kaynakların verimli bir şekilde tahsisini iyileştirmeye yardımcı olmaktadır. Akıllı şehir sistemlerinin mimarisi, bağımsız-heterojen ağ ve altyapıların birbirleriyle bağlantılarından oluşmaktadır. Cihazlar, iletişim teknolojileri, ağ protokolleri ve platformlar bakımından heterojen yapıda olan bu mimari ve ağların birlikte çalışabilirliği, üzerinde durulması gereken bir tasarım problemidir. Mevcut yaklaşımlarda merkezi bir yönetim katmanı ile farklı kaynaklardan gelen verilerin toplanması, organize edilmesi, analizi ve depolanması ile akıllı karar verme işlemleri gerçekleştirilir. Bu yapıdaki yaklaşımlarda ana problem, bu boyuttaki veri yükünü merkezi bir noktadan idare etmeye çalışmanın verimsizliği ve işlemlerde yaşanan gecikmelerdir. Problemleri ortadan kaldırarak daha etkili ve verimli bir veri işleme gerçekleştirme için dağıtık veri işleme metodlarından yardım alınmalıdır. Dağıtık yaklaşımda ağdaki karar verme işlemleri dağıtık bir şekilde gerçekleştirilerek ağlar ya da cihazlar arasında birlikte çalışabilirlik yoluyla iletişim desteklenir.

Akıllı şehir sistemlerinin en önemli parçalarından biri olan ve verinin sensör düğümler ya da katılımcılar yardımıyla toplandığı IoT ağlarında, sunucu merkezli mevcut iletişim modelinin yerine verinin odakta olduğu veri merkezli yaklaşımın kullanılabilmesi için tasarlanmış bilgi merkezli ağ haberleşmesi yaklaşımının kullanılması gerekmektedir. Bu yaklaşımın en çok kullanılan çeşidi adlandırılmış ağ haberleşmesidir. Adlandırılmış ağ haberleşmesi mimarisi eşsiz içeriği adlandırarak, yaygın ön belleğe alan, doğal bir akış kontrolüne sahip, toplama tabanlı bir iletişim mimarisidir. Yapılan çalışmalar bu veri merkezli yaklaşımın, IoT uygulamalarının kendine özgü üretici/tüketici tabiatı ile ağ operasyonlarını düzenlediğini ve de IoT ağları için mükemmel uygunlukta olduğunu göstermektedir.

Geleneksel merkezi veri işleme sistemlerinde bulunmayan ölçeklenebilir olmak, yüksek uygunluğa sahiplik, hata toleransı yeteneği gibi kritik özellikler dağıtık veri işleme mekanizmaları ile mümkün hale gelmiştir. Dolayısıyla bu özelliklere ihtiyaç duyan akıllı şehir sistemleri ve uygulamalarının bu avantajdan yararlanabilmesi için dağıtık veri işleme mekanizmalarını sistemlerinin bir parçası haline getirmesi yerinde olacaktır. Ülkemizde yapılacak olan akıllı şehir sistemlerinde de verinin dağıtık olarak işlenmesi, bu veri işleme yönteminin getirdiği hızlı işlem özelliği, otonom ağlar arası bağlanabilirlik ve iletişim gibi avantajlardan yararlanılmasını sağlayacaktır. Dağıtık veri işleme modelinin seçiminde paydaşlarla beraber bölgesel ve ulusal ihtiyaçlar ile altyapı imkân ve özelliklerinin dikkatli bir şekilde analiz edilmesi, gerekli altyapı çalışmalarının yapılarak ağ altyapısı ile uyumlu bir şekilde çalışacak bir modelin oluşturulması gerekmektedir. Bölgeler ve otonom ağlar arasındaki veri paylaşımına ilişkin kuralların ve tarafların sorumluluklarının açıkça belirlenmesi faydalı olacaktır. Ortak mekanizmaların ve mimarinin belirlenmesi ve tasarlanması hem ulusal hem de bölgesel olarak çalışmaların sürdürülebilirliği açısından önem arz etmektedir.

KAYNAKLAR

T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, 2021. Dağıtık Veri İşleme/ <https://www.akillisehirler.gov.tr/egitim-dagitik-veri-isleme/>, (Eylül 2022).

Bawany N. Z., Shamsi J. A. (2015). Smart city architecture: Vision and challenges. International Journal of Advanced Computer Science and Applications, 6(11).

- Birleşmiş Milletler** (2018), 2018 revision of world urbanization prospects Erişim Adresi: <https://population.un.org/wup/Publications/Files/WUP2018-Report.pdf>.
- Atzori, L., Iera, A., Morabito, G.** (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.
- Datta, S. K., Bonnet, C., Haerri, J.** (2015). Fog computing architecture to enable consumer centric internet of things services. In 2015 International Symposium on Consumer Electronics (ISCE) (pp. 1-2). IEEE.
- ETSI, M.** (2014), Mobile edge computing Erişim Adresi: https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf.
- Tourani, R., Mtibaa, A., Misra, S.** (2019). Distributed data-gathering and processing in smart cities: An information-centric approach. *Open Journal of Internet Of Things (OJIOT)*, 5(1), 93-104.
- Silva, B. N., Khan, M., Han, K.** (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*, 38, 697-713.
- Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., Braynard, R. L.** (2009). Networking named content. In Proceedings of the 5th international conference on Emerging networking experiments and technologies (pp. 1-12).
- Bouk, S. H., Ahmed, S. H., Kim, D., Song, H.** (2017). Named-data-networking based ITS for smart cities. *IEEE Communications Magazine*, 55(1), 105-111.
- Mick, T., Tourani, R., Misra, S.** (2017). LAsER: Lightweight authentication and secured routing for NDN IoT in smart cities. *IEEE Internet of Things Journal*, 5(2), 755-764.
- Piro, G., Cianci, I., Grieco, L. A., Boggia, G., Camarda, P.** (2014). Information centric services in smart cities. *Journal of Systems and Software*, 88, 169-188.
- Zhang, L. vd.,** (2014). Named data networking. *ACM SIGCOMM Computer Communication Review*, 44(3), 66-73.