

YENİ NESİL AKILLI ŞEHİR MİMARİSİNDE GÜVENLİ ÇOK TARAFLI HESAPLAMA UYGULAMALARI

Alper OZPINAR¹, Hüseyin BAYRAKTAR², Dursun Yıldırım BAYAR³, Gökhan BİLGİN⁴

¹Dr. Alper Özpinar, İstanbul Ticaret Üniversitesi, Mekatronik Mühendisliği Bölümü, Maltepe, İstanbul, aozpinar@ticaret.edu.tr

²Dr. Hüseyin Bayraktar, Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, huseyin.bayraktar@csb.gov.tr

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

⁴YGökhan BİLGİN, Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, gokhan.bilgin@csb.gov.tr

ÖZET

Akıllı Şehirler kavramı insanoğlunun yakın geleceğine ev sahipliği yapacak uzaya açılmadan önce dünya üzerindeki daimi yaşam alanları olacak bir kavram olmaktadır. Akıllı şehirler önümüzdeki yüzyılın sosyal ve beşeri yaşamının altyapısını kuracak ve yeni bir yaşam yaklaşımında çok önemli bir rol oynayacaktır. Akıllı şehir kavramı onu oluşturan öncelikle içinde yaşayan, çalışan, ziyaret eden insanlar ile o insanlara hizmet ve servis sağlayan tüm kurum, değer ve varlıkların iş, veri, uygulama ve teknoloji katmanında tek bir bütünlüklü yapıda bir ekosistem oluşturması ile oluşabilecektir. Bu kadar karmaşık bir ekosistemin doğru yönetilebilmesi ve uyum içerisinde olabilmesi için iş, veri ve süreç modellerine sahip olması gerekmektedir. Akıllı Şehir mimarileri içerisinde bu ekosistemin bu karmaşıklık içerisinde bir kaos oluşturmaması için en üst düzeyde iletişim ve gerekli veri paylaşımına sahip olması, bu verilerin yetkiler kapsamında işlenmesi ve kullanılabilmesi gerekmektedir. Bu kadar büyük verinin işlenebilmesi özel güvenlik ve yetkilendirme şemalarına ihtiyaç duymakta, veri işleyicilerin yetkisi oranında veriye erişebilmesi ve kullanabilmesi gerekmektedir. Ancak günümüzde bulut bilişim, yüksek hesaplamalı bilgisayarlar, dağıtık hesaplama, farklı paydaşların veriye erişme ihtiyaçları yeni nesil veri işleme ve analiz yöntemlerine olan ihtiyacı da oluşturmaktadır. Verinin mahremiyeti kadar paylaştıkça güvenliğinin azalmasına rağmen rekabetçi ortamda akıllı şehir uygulamaları içerisinde verileri açık olarak paylaşmadan şehre hizmet için istatistik ve analiz hesaplarında kullanılabilmesi ihtiyacına yönelik olarak bilgi teknolojileri alanında da yeni algoritmaları ve şifreli hesaplama yöntemleri geliştirilmektedir.

Bu makalede yüksek güvenli ve çok taraflı hesaplama ihtiyacı duyulan akıllı şehir bileşenleri içerisindeki ulaşım, sağlık, eğitim gibi alanlardaki uygulamalar incelenmiş ve modele uygunlukları kavramsal olarak test edilmiştir. Makalede ulaşım, sağlık ve eğitim alanlarında güvenli çok taraflı uygulama yaklaşımına uygun veri setleri, veri alanları ve veri tipleri anlatılmış ve modellenmiştir.

Anahtar Sözcükler: Akıllı Şehirler, Güvenli Çok Taraflı Hesaplama, Büyük Veri, Bulut Bilişim, Veri Paylaşımı ve İşleme.

ABSTRACT

SECURE MULTI PARTY COMPUTATION APPLICATIONS IN NEXT GENERATION SMART CITY ARCHITECTURE

The concept of Smart Cities will be one that will be permanent living spaces on Earth before opening up into space that will house the near future of humans. Smart Cities will create the infrastructure for social and human life in the next century and will play a very important role in a new way of life. The concept of a smart city can be formed by creating an ecosystem with a single integrated structure at the business, data, application, and technology levels of the people who live, work, and visit there, as well as all the institutions, assets, and values that provide services to those people. For such a complex ecosystem to be properly managed and harmonized, it must have business, data, and process models. In order for this ecosystem not to create chaos among smart city architectures in this complexity, it should have the highest level of communication and necessary data exchange, and this data should be processed and used in the context of permissions. Processing such big data requires specific security and authorization schemes, and data processors must be able to access and use the data within the scope of their authority. However, cloud computing, high-performance computing, distributed computing, and the data access requirements of various stakeholders today also necessitate a new generation of data processing and analysis methods. In the field of information technologies, new algorithms and encrypted computation methods are being developed to meet the need to use data for statistical and analytical computations in the service of the city without openly sharing the data in smart city applications in a competitive environment, although the privacy of the data decreases with sharing.

In this article, applications in areas such as transportation, health, and education in smart-city components that require highly secure multilateral data processing are explored, and their suitability for the model is conceptually examined. The article explains and models datasets, data fields, and data types that are suitable for a secure multilateral application approach in the areas of transportation, health, and education.

Keywords: Smart Cities, Secure Multi Party Computation, Big Data, Cloud Computing, Data Sharing and Processing

1. GİRİŞ

Akıllı şehirler kavramı 1970’lerde Amerika Birleşik Devletleri’ndeki Los Angeles şehrindeki ilk büyük veri projesi ile konuşulmaya başlanmıştır; sonrasında 1994’de Hollanda Amsterdam’daki “Dijital Şehir” kavramı ile internet ile buluşmuş; ilerleyen yıllarda ise teknoloji ve donanım üreticileri Cisco ve IBM gibi firmaların konu ile ilgili yaptıkları çalışmalarla birlikte 2000’li yıllardan itibaren hayatımızda ve şehircilik kavramı içerisinde yer olmaya başlamıştır. (Global Data Thematic Research, 2020)

Bilgi ve İletişim Teknolojilerinin özellikle son yirmi yıl içerisinde erişilebilirlik ve maliyet olarak yaygınlaştırılabilir olması hem de sürdürülebilir bir akıllı şehirler kavramı içerisinde kentsel sorunlara ve gündelik ihtiyaçlara daha etkin olarak fayda sağlar hale gelmiştir. Farklı kurum ve firmaların kendi çözüm alanları ve yetkinliklerine göre akıllı şehirler kavramına sağladıkları faydalar ve çözümler bulunmasına rağmen uçtan uca bir akıllı şehirler ekosistemini tek başına karşılayabilecek bir entegre çözüm çok olası görülmemektedir. Akıllı şehirler teknolojileri olarak adlandırılan bu teknolojiler sunmakta olan global şirketler, akıllı şehirler ve paydaşları ile kavram ispatı olarak da tanımlanabilecek pilot çalışmalar ile bu pazarda kontrolü sağlamaya çalışmaktadırlar. (van den Buuse & Kol, 2019)

Türkiye’nin de içinde bulunduğu Avrupa Birliği coğrafyasında ise Avrupa Birliği süreçleri kapsamında çalışmalar ve projeler yürütülmektedir. (Caragliu vd., 2011) Geçmiş yıllarda akıllı şehirler ile ilgili projeler genel olarak akıllı şehirler altyapılarına yönelik teknoloji güncellemesi ve yoğun olarak kentsel altyapı yatırımları olarak yapılırken, son yıllarda bu yaklaşım yerini akıllı şehir servisleri ve bunların işletilmesi, bakımı ve sürdürülebilir olmasına yoğunlaşmıştır. (Kim, 2022)

Akıllı şehir servisleri ile ilgili en önemli ve vazgeçilmez olan bileşen ise “şehir verisi” olarak da tanımlayabileceğimiz, akıllı şehir kavramı ile ilgili tüm paydaş vatandaş, kurum, şirketlere ve akıllı şehir servis ve hizmetlerine dair verileri kapsamaktadır. Akıllı şehir verileri yapısal ve boyutsal olarak büyük veri olarak tanımlan kategoriye girmektedir. Büyük veri boyutları olan ve İngilizce 5V olarak tanımlanan verinin oluşma, toplanma ve saklanmasına dair çeşitlilik (variety), hacim (volume), hız (velocity), doğruluk (veracity), değer (value) boyutlarından oluşmaktadır. Büyük veri ile ilgili ilk tanımların yapılmaya başladığı ve sanallaştırma sistemlerinin yavaş yavaş yaygınlaşmaya başladığı bulut bilişim kavramının iş dünyası için ticari uygulamalara dönüştüğü 2010’lu yıllarda ana kavram aslında biraz da akıllı şehirler gibi bu verinin altyapısına dair çalışmaları içermekteydi. Bu nedenle ilk büyük veri tanımları 4V olarak yapılmış işin içine bu verinin hangi servisler ve hizmetler kapsamında katma değer oluşturacağı düşünülmemiştir. Sonrasındaki yıllarda bu kadar büyük verinin sadece toplanması değil bunun bir değere dönüşmesinin stratejik önemi anlaşılmıştır. 2020’li yıllara kadar yapılan bir çok makale çalışmada büyük veri 4V olarak tanımlanmaktadır. (al Nuaimi vd., 2015; Lin vd., 2017; Shu, 2016) Büyük veri kavramı akıllı şehirler içerisinde de çok önemli ve kritik bir role ve misyona sahiptir. (Hashem vd., 2016) Bu büyük veriler sayesinde akıllı şehirler, sağlık, ulaşım, enerji, eğitim ve su hizmetlerinin performansını iyileştirmek için birden fazla teknolojiyi kullanarak vatandaşlarının daha yüksek konfor seviyelerine ulaşmasını sağlayabilmektedir. (al Nuaimi vd., 2015)

Günümüzde ise veri artık yeni bir ekonomik model haline gelmiş ve 20. Yüzyılın hakim petrol ekonomisinin yerine geçmiştir. (Javornik vd., 2019) “Veri, yeni petroldür” kavramını, beraberinde verinin petrol gibi dolaşımda olması, veri paylaşımı ekonomisi gibi kavramlar da gelişmeye başlamıştır. (Richter & Slowinski, 2019) Verinin, bir varlık olarak değerlendirilmesi, (Birch vd., 2021) , bu varlığın bir emtia gibi alınıp satılabilmesi (Aaltonen vd., 2021) ve tabiki veri analizi, veri madenciliği veriye dayalı yapay zeka algoritmalarının oluşturduğu katma değerli hizmetler (Gupta vd., 2019) yeni nesil yaklaşımları da beraberinde getirmiştir.

Özellikle yapay zeka, makine öğrenmesi ve derin öğrenme uygulamalarının insana dair tüm süreçlerin içinde olması neticesinde akıllı şehirler servis ve hizmetleri de bu kavramların ışığında güncellenmiş ve gelişmeye başlamıştır. (Allam & Dhunny, 2019) Bu verilerin kaynağı olan uygulamalar, sensör teknolojileri ve IIoT olarak tanımlanan endüstriyel nesnelerin interneti donanımları ile bu verilerin çeşitliliği ve büyük veri yetkinlikleri artmıştır. (Bibri, 2018; Hajjaji vd., 2021)

1.1 Akıllı Şehir Mimarileri

Akıllı şehirler kavramı içerisinde bir çok bilgi ve iletişim teknolojileri altyapısı ve çözümü bulunduğundan tüm bu bileşenlerin uyum içerisinde çalışabilmesi için uygun bir mimari yaklaşım içerisinde tanımlanması gerekmektedir. Literatürde mimari, modelleme, tasarım kelimeleri çok yakın anlamlar ve benzerlikler içermektedir. Bilgi ve iletişim teknolojileri kavramlarının kurumsal yaklaşımı içerisinde değerlendirildiğinde bir çok yakın kavram ortaya çıkmaktadır; kurumsal mimari (enterprise architecture), kurumsal modelleme (enterprise modelling), kurumsal tasarımsal düşüncesi (enterprise design thinking), kurumsal yazılım tasarımları (enterprise software design) ve kurumsal entegrasyon (enterprise integration) gibi kavramlar çok farklı bakış açılarından değerlendirilebilmektedir. (D. Chen vd., 2008) Bu kavramlar özellikle pratik yazılım mühendisliğine yönelik yazılım mimari ile de sıklıkla karıştırılabilmekte ve beklentiler açısından uyumsuzluklar yaratabilmektedir. (Chung & Subramanian, 2007)

Akıllı şehir mimarileri ile Akıllı Şehir kavramı içerisinde yer alan varlıkların iş, veri, uygulama ve teknoloji katmanında tek bir bütünleşik yapıda yönetilebilmesi ve uyum içerisinde çalışabilecek iş, veri ve süreç modellerini kapsaması olarak ele alındığında bu tip karışıklıkların önüne geçmek mümkün olabilir. Bu çalışmada akıllı şehir mimarileri içerisinde yeni nesil veri paylaşımına yönelik çok taraflı hesaplama uygulamalarına ilişkin örnekler aktarılacaktır.

1.2 Akıllı Şehir Uygulamalarında Veri ve Veri Güvenliği

Günümüzde veriye erişebilmek ve bu veriyle yapılabileceklerin farkında olmak sektör fark etmeksizin bütün kurumlar için büyük önem taşımaktadır. (Özpınar vd., 2021) Bu verilerin kaynağı akıllı şehir bileşenleri olduğunda bu veri ile neler yapılabileceği, ne tür hizmetler sağlanabileceği gibi toplum için ne tür faydalar sağlanabileceği her geçen gün artmakta ve çeşitlenmektedir. Ancak veri ekonomisi içerisinde verinin bir değerli varlık olmasından kaynaklı korunması, erişiminde kural ve denetim mekanizmalarının tanımlanması gerekmektedir. Teknolojinin kural ve yönetmeliklerden çok daha hızlı geliştiği ve evrildiği günümüzde etik kavramlar ile birlikte insan odaklı akıllı şehir çözümlerine yönelik geliştirmelerde güvenlik ve risk kavramları da ortaya çıkmaktadır. İnsan refahını ve sosyal gelişmeyi kolaylaştırmak ve geliştirirken tehdit ve risk oluşturulmaması hedeflenmektedir. (Ahmad vd., 2022) Özellikle eğitim (Alexei & Alexei, 2021; Hina & Dominic, 2020; Ulven & Wangen, 2021), sağlık (Islam vd., 2015; Li vd., 2013), enerji (Clastres, 2011; Jacobson, 2009; Ni vd., 2018) ve özellikle ulaşım hizmetleri (Papastergiou vd., 2021; Rausand & Haugen, 2020; Tonn vd., 2019; Wang & Zhang, 2020) gibi alanlarda veri güvenliği ve veriler yönelik siber saldırı riskleri bulunmaktadır. Veri sadece bir hedef değil aynı zamanda korunması gereken bir varlıktır.

Özellikle akıllı şehir uygulamaları içerisindeki kişisel verilerin KVKK uyumlulukları, kişisel verilerin korunması gibi konular verilerin paylaşılması ve uygulamalar içerisinde kullanılması ile birlikte farklı bir korunma ihtiyacı oluşturmuştur. Verilerin toplanması ve işlenmesi ile ilgili Avrupa Birliği içerisinde GDPR olarak da bilinen “Genel Veri Koruma Yönetmeliği” bireyler için veri koruma ve gizliliğine dair tanımları yapmış olsa da, pratik uygulamalarda ortaya çıkan ihtiyaçlar ve durumlar bu yönetmeliğin tüm sorulara cevap veremediğini ortaya koymaktadır. (Mazzi vd., 2021) Özellikle ticari işletmelerin veri toplamak için yaygın olarak kullandıkları sadakat programları uygulamaları, ticari olarak kişisel verileri toplayan ve işleyen şirketlerin ilk örnekleri olarak gösterilmektedir. (Alizadeh vd., 2019) Günümüzde kişisel bilgiler her türden şirket tarafından çok çeşitli amaçlarla her zamankinden daha fazla kullanılmakta bu verilerin akıllı şehir uygulamalarına yönelik yansımaları ise her geçen gün artmaktadır. Özellikle lokasyon bazlı servisler ile bireylerin şehir içerisindeki hareketlilikleri, ulaşım kullanımları, alışveriş tercih ve rotaları, araç kullanım istatistikler, toplu taşıma tercihleri gibi verilerin toplanması ve kullanımının her geçen gün artmasına neden olmaktadır. (Usman vd., 2018) Akıllı şehir servis ve hizmetlerinin daha kapsamlı ve karmaşık olması ise bütünleşik hizmetler olarak da tanımlayabileceğimiz birden çok kurum ve işletmenin dahil olduğu hizmetleri kapsamaktadır. Bu konu ile ilgili birçok akademik çalışma ve ticari örnek bulunmaktadır. Özellikle hizmetlerin dağıtık ve servis olarak verilebilmesi ticari olarak da sürdürülebilir olmasını sağlamaktadır. (Anthony vd., 2020; Schaffers vd., 2011; Voorwinden, 2021)

Farklı kurum ve işletmelerin ortak servis ve hizmet verebilmesi için birbirleri arasında sınırları ve kuralları dahilinde veri paylaşımı ve veri alışverişi yapmaları gerekebilmektedir. Veri paylaşımı için web servis tabanlı bir çok teknolojik imkan bulunmakta ve bu tip servislerin kullanımı her geçen gün artmaktadır. Ancak günümüzde bu tip veri paylaşımı daha çok bireyin kendi talebine yönelik olarak yapılmakta ve özellikle satın alınan bir hizmet ile ilgili ek servis ve hizmetlerin alınmasına yönelik paylaşımlar odağında olmaktadır. Örneğin bir havayolu şirketinden uçak rezervasyonu yapmak istediğinizde bu rezervasyon ile birlikte otel ve araç kiralama hizmetlerinin de size sunulması gibi sınırlı bir ürün sorgusu özelinde veri paylaşımı yapılmaktadır, bu veriler daha çok kişisel verilerden ziyade alınacak hizmete yönelik sorgular bazında olmaktadır. Müşteri ek servisleri almak istediğinde ise sistemler arasında veri transferi ve aktarımı yapılmaktadır. Ancak bu tip yaklaşımlar kısa süreli ve anlık olarak yapıldığından daha çok sürekli veri akışına yönelik değildir. Ancak özellikle ödeme sistemleri ile ilgili kampanyalar yapan bankaların kredi kartı özelinde sundukları ek indirim ve hizmetler (Ding vd., 2018; Laidroo & Avarmaa, 2020) ile GSM şirketlerinin lokasyon bazlı indirim ve hizmetlerine yönelik uygulamalarında lokasyon bazlı veri paylaşımları yapılabilmektedir. (Giannotti vd., 2007)

Tüm bu bilgiler ışığında verilerin korunması, güvenli olarak saklanması ve gerektiğinde uygun bir şekilde kullanılabilmesine yönelik teknolojik ve akademik çalışmalar da son yıllarda artmıştır. Verilerin korunmasına ve güvenli olarak aktarılmasına yönelik şifreleme algoritmaları, çözümleri ve donanımları günümüz bilgi teknolojileri dünyasının ayrılmaz bir parçası olmuş durumdadır. (Bethencourt vd., 2007; Goyal vd., 2006; Lamport, 1981; Needham & Schroeder, 1978)

Bu çalışmanın ilerleyen bölümlerinde güvenli şifreleme ve veri aktarımı konularından ziyade verinin güvenli bir şekilde farklı kurum ve kuruluşlar tarafından verinin mahremiyetinin bozulmadan işlenebilmesi konusunda değerlendirmeler yapılacaktır.

1.3 Güvenli Çok Taraflı Hesaplama Yöntemleri

Farklı uygulama ihtiyaçlarına yönelik olarak birden çok veri işleyicisinin aynı yada farklı veriler üzerinde yapacakları hesaplama işlemleri için geliştirilen Güvenli Çok Taraflı Hesaplama (Secure Multi Party Computation) ya da Mahremiyeti Koruyan Hesaplama (Privacy Preserving Calculation) yaklaşımları özellikle yüksek başarımli hesaplama sistemlerinin geliştirilmesi, bireysel bilgi teknolojileri donanımlarının hesaplama güçlerinin artması, yüksek hızlı internet erişimi üzerinden bulut bilişim servisleri üzerinden yüksek performanslı sistemlerin servis olarak kullanılabilirdiği hizmetlere erişilebilmesine imkan bulunması sonrasında yaygınlaşmaya başlamışlardır.

Veri analizi, veri istatistiği, makine öğrenmesi amaçlı veriyi oluşturan nümerik veri boyutları üzerinde analitik odaklı hesaplama yapmak isteyen ancak bu veriler doğrudan erişmeye yetkisi olmayan veya KVKK gibi süreçler nedeni ile verilerin maskelendiği gizlendiği durumlarda verilerin mahremiyetine zarar gelmeden işlem yapabilmesi kavramına dayanan bu yaklaşımda geleneksel şifreleme ve iletişim yöntemleri yeterli olamamaktadır.

Bir önceki bölümde aktarıldığı üzere veriler üzerinde farklı yetkilerde erişim sağlanabilmektedir. Bu erişim yetkileri okuma, yazma, güncelleme ve silme olarak da bilinen temel veri tabanı işlemleri olarak tanımlanmaktadır. Ancak verilerin hesaplamlarda kullanılması için öncelikle verilerin okunabilmesi ihtiyacı bulunmaktadır. Paydaşların veriler üzerinde kendi kurumlarına özel alınmış veri işleme ve kullanma yetkileri olabilmemesine rağmen bu yetkiler verilerin kurum dışında farklı paydaşlar tarafından da işlenebilmesine yönelik bir izin vermemektedir.

Çok uluslu teknoloji şirketlerinin özellikle sosyal medya uygulamaları üzerinden bu tip izinleri alma çalışmaları ise farklı tepkiler alabilmektedir. Örneğin en büyük beş bilgi teknolojileri şirketleri arasında yer alan Facebook firmasının (Gautier & Lamesch, 2021) 2014 yılında şirket portföyüne kattığı mesajlaşma uygulaması Whatsapp üzerinden (Saha vd., 2021) toplanan verilerin şirket portföyündeki diğer uygulamalar ve firmalar ile paylaşılabileceğine yönelik güncelleme sonrasında bir çok farklı alternatif uygulamaya yönelmişler sonrasında firma bu veri paylaşımı ile ilgili ek açıklamalar yapmak durumunda kalmıştır. Bireylerin her gün kullandıkları bir çok uygulamada farkında olmadan paylaştıkları birçok veri bulunmasına rağmen toplumsal bir hareket sonucunda tepkiler daha hızlı oluşmuştur. Bu konular ile ilgili de bir çok farklı veri ve bilgi kirliliği de oluşmakta, özellikle internet üzerinden Hoax olarak tanımlanan aldatıcı mesajlar, sahte haberler, söylentiler ile veri paylaşım ve güvenliği konusu farklı boyutlara ulaşmıştır. (Meel & Vishwakarma, 2020)

Tüm bu gelişmeler ışığında günlük yaşamda yoğun olarak kullanılmakta olan bir mesajlaşma uygulamasının sadece uygulamayı geliştiren şirketin iştirakleri ile veri paylaşacak olması bile ciddi bir etki yaratmıştır. Bu kapsamda akıllı şehir uygulamaları içerisinde bir çok ticari olarak rekabet içerisinde olan kurum ve şirketin bu tip verilere olan ihtiyacı ve bu tip verilerin bütünsel hizmetler içerisinde katma değerli servisler olarak kullanılabilmesi yeni nesil dijital ekonominin en önemli ürünlerinden biri haline gelmektedir.

Tüm bu gelişmeler ışığında verilerin güvenli bir şekilde mahremiyeti ihlal etmeden matematiksel olarak güvenliği oluşturulmuş algoritmalar ile korunarak sınırlandırılmış amaç ve hizmetlere uygun olarak işlenebilmesine yönelik ihtiyaç da aynı oradan artmıştır.

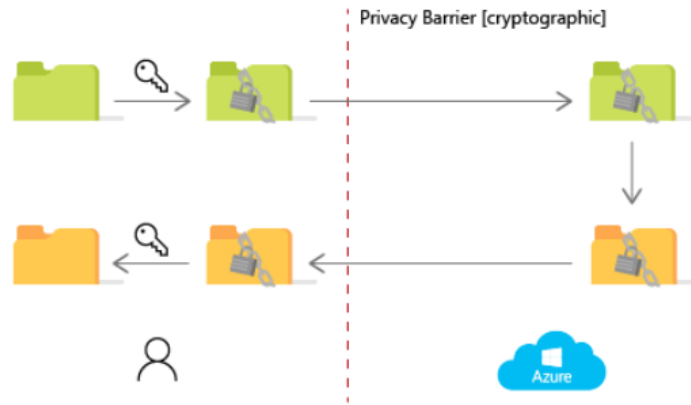
Bu konuda yapılan ilk çalışmalar aslında bilgi ve veri güvenliği kavramlarının internet üzerinden yaygın olarak kullanılması, toplanması ve işlenebilmesinden çok önce kavramsal olarak tartışılmıştır. 1930'larda oyun teorisi ile ilgili teorilerin gelişmesinde önemli bir rol oynayan bulmaca ve oyunların çözüm algoritmaları çalışmaların benzer olarak (Barnett, 2009), 1970'lerde birbirlerinden fiziksel olarak uzak mesafedeki oyuncuların güvenli ve adaletli bir şekilde kart oyunları oynayabilmelerine imkan veren poker oynama algoritması özellikle şifreleme ve şifreli veri paylaşımı konusunda bir çok çalışmaları da bulunan yazar tarafından geliştirilmiştir. (Shamir, 1979; Shamir vd., 1981)

Sonrındaki yıllarda güvenli ortak hesaplama (A. C. Yao, 1982a) ve güvenli bir şekilde gizli verilerin paylaşılabilmemesine yönelik (A. C. C. Yao, 1986) çalışmalar yapılmıştır. (A. C. Yao, 1982b) Ancak tüm bu çalışmalar verilerin kısıtlı ve paylaşım imkanlarının az olduğu 2000'li yıllar öncesinde önerilen algoritmaların ihtiyaç duyduğu yüksek iletişim ve hesaplama altyapısının pratik olarak karşılanamaması ve uygulamada verimsiz olmalarından dolayı yoğun bir ilgi ve geliştirmeyi görememiştir.

Ancak ilerleyen yıllar içerisinde veri mahremiyeti, çok taraflı tekliflendirme uygulamalarının yaygınlaşması bu konuda homomorfik şifreleme algoritmasının da hesaplamlarda kullanılabilmesi ile (Damgård vd., 2012; Rivest vd., 2001) yeni bir uygulama ve iş modelleri geliştirilebilmiştir.

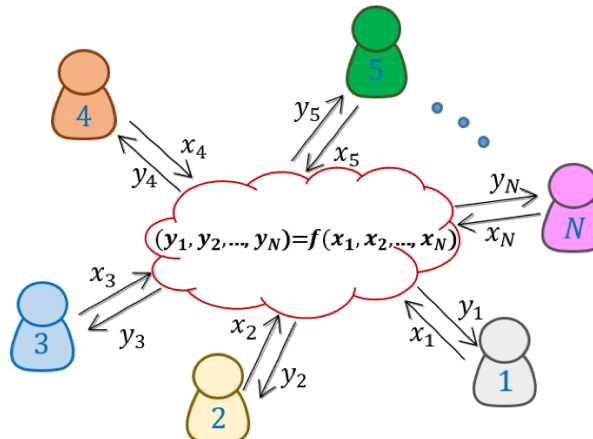
Güvenli çok taraflı hesaplama modelleri ve buna bağlı şifreli veri ile çalışabilme kavramları aslında iki ana konu üzerinde yoğunlaşmaktadır. Bu konular özellikle makine öğrenmesi gibi güncel veri analizi yöntemleri özelinde geliştirilmektedir. (Jiang vd., 2020)

- Homomorfik Şifreleme ile verilerin şifreli bir şekilde işlemlerde kullanılması ve hesaplamaları yapan taraflarında verinin açık halini görmeden bazı işlemleri gerçekleştirebilmesini sağlar. Bu yöntem ile aslında veriler tamamen şifrelenmiş olduğundan maskelenmesi, gizlenmesi yada açık veri gibi davranılmasına gerek yoktur. Şifreli veriler üzerinden yapılacak tüm hesaplamalarda verinin mahremiyeti korunmuş olacaktır. Verilerin bütünlüğü ve gizliliğinin korunduğu bu yaklaşımda verinin sahibi verisini istediği ortamda desteklenen algoritma ve hesaplama yöntemleri dahilinde işleyebilir. Verinin işlendiği yer ve kurum veriler üzerinden hiçbir bilgiyi göremez yada açığa alıp kullanamaz. Bu amaç için kullanılmakta olan en yaygın algoritmalar ve kütüphaneler BFV (Fan & Vercauteren, 2012), Microsoft SEAL(H. Chen vd., 2017; Cui vd., 2020), HEAAN algoritması (Cheon vd., 2018, 2019; Cui vd., 2020) , IBM HeLib (Halevi & Shoup, 2014, 2020) olarak özetlenebilir. Bu çalışmada uygulama olarak SEAL algoritmasının açık kaynak kodlu olan Python dilinde geliştirilmiş olan TenSEAL paketi kullanılmıştır.(BenaissáBenaissá Ecole Supérieure en Informatique vd., 2021) Microsoft firması SEAL algoritması ile ilgili olarak bulut bilişim servisleri Azure üzerinden bu hizmetin de büyük uygulamalar için barındırma ve hesaplama hizmetini sağlayabilmektedir. (Şekil 1) Matematiksel işlemlerin tam anlamı ile yapılabildiği Tamamen Homomorfik Şifreleme olarak tanımlanan FHE ile kısıtlı işlem kütüphanesi daha etkin işlemler için kullanılabilir.



Şekil 2. Microsoft SEAL Algoritması Bulut Hizmeti.

- Güvenli Çok Taraflı Hesaplama ile birden çok paydaşlı veri kaynağı verilerini birbirleri ile doğrudan açık verileri paylaşmadan tanımlı istatistikî yöntemler ve matematiksel fonksiyonlara gizleyerek ortak hesaplamalarında kullanabilirler. (Şekil 2) Bu yöntemde benzer veri üreten ve işleyen kurumlar sistemin bütününe dair hesaplamaları paylaşımcı olarak mahremiyeti bozmadan kullanabilirler. (Zhao vd., 2019) Bu hesaplamalar için yine açık kaynak kodlu SyMPC kütüphanesinin fonksiyonları değerlendirilmiştir. (GitHub - OpenMined/SyMPC: A SMPC Companion Library for Syft, t.y.) Güvenli çok taraflı hesaplama ile benzer içerikleri kullanan ama verilerin paylaşımından ziyade makine öğrenmesi parametrelerinin ve öğrenim modellerinin paylaşıldığı federe öğrenme yaklaşımlarının da kullanılması mümkündür. Bu yaklaşım için de yine benzer şekilde açık kaynak kodlu PySyft kütüphanesi değerlendirilmiştir. (Ziller vd., 2021)



Şekil 2. Güvenli Çok Taraflı Hesaplama Algoritması.(Lemus vd., 2020)

2. UYGULAMA

Bu çalışmada akıllı şehir uygulamaları içerisinde veri hesaplamaları ve veriye dayalı makine öğrenmesi algoritmalarına yönelik olarak uygulamalara yönelik akıllı şehir hizmetlerine yönelik olarak akıllı ulaşım, akıllı sağlık ve akıllı enerji özelinde örnekler tanımlanmıştır. Uygulama örneklerine ilişkin analiz ve simülasyonlar için kullanılan veri setleri ve detaylı veri yapıları uygulama özelinde verilmiştir. Her bir alt başlık ile ilgili olarak homomorfik şifreleme ve güvenli çok taraflı hesaplama kapsamında ki paydaşlar ve veriler tanımlanmıştır. Akıllı şehir tanımları, örnek uygulama ihtiyaçları ve paydaşlara ilişkin bilgiler ve örnekler Çevre Şehircilik ve İklim Değişikliği Bakanlığının internet sitesinden alınmıştır. (*AKILLI ŞEHİRLER – 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*, t.y.)

Uygulama kapsamında genel olarak homomorfik şifreleme ile yapılabilecek yüksek performanslı hesaplama taleplerinin bulut bilişim yada akıllı şehir hizmet sunucuları olarak atabilecek sunucularda hesaplanabildiği yaklaşımlar düşünülmektedir. Bu çalışmalar kapsamında veri sahibi verisini şifreli bir şekilde bu sunuculara gönderecek yazılım sistemi üzerinden gönderir ve yapılması hedeflenen hesaplama algoritmalarının çalışması sonrasında sonucu yine şifreli olarak aldıktan sonra güvenli olan paylaşımsız kendi cihazı üzerinde sonucun şifresini çözebilir. Bu yaklaşımlar özellikle optimizasyon amacı ile kullanılabilecek farklı alternatifleri değerlendirilmesini sağlayabilecek sezgisel ve geleneksel algoritmalar için kullanılabilir. (Farokhi vd., 2020) Benzer şekilde sağlık ve enerji uygulamaları için de yaklaşımlar kullanılabilir. (Munjal & Bhatia, 2022)

2.1 Akıllı Ulaşım

Tanım : Akıllı ulaşım, Bilgi ve İletişim Teknolojileri destekli ve entegre ulaşım sistemleridir. Bir veya birden fazla ulaşım şeklinin kullanıldığı tramvay, otobüs, tren, metro, araba, deniz ve hava ulaşımını, bisiklet ve yayaları kapsayan sürdürülebilir, güvenli ve birbirine bağlı ulaşım sistemlerini kapsamaktadır. (*AKILLI ŞEHİRLER – 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*, t.y.) Uygulama matrisi Çizelge 1’de verilmiştir.

Çizelge 1. Akıllı Ulaşım Hesaplama Uygulamaları Matrisi.

Örnek Uygulama	Homomorfik Şifreleme	Güvenli Çok Taraflı Hesaplama
Otopark Dinamik Fiyatlandırma	Fiyat optimizasyonu	Otoparklar arası arz/talep hesaplaması
Otopark Doluluk Tespiti	Bulut tabanlı görüntü işleme uygulaması	Otoparklar arası doluluk ve araç istatistik uygulaması
Yoğunluk Algılayıcı Sensörler	Sensör füzyonu derin öğrenme ve bakım uygulaması	Sensör veri istatistikleri uygulaması
Gerçek Zamanlı ve Dinamik Kavşak Yönetim Sistemleri	Trafik sinyalizasyon optimizasyonu	Kavşak doluluk bilgileri paylaşımı
Kişiselleştirilmiş Ulaşım Bilgileri	Rota-zaman-tercihli yol sezgisel algoritmalar kullanımı	Servisler arası yolcu istatistikleri uygulaması
Yolculuk Planlama	Bulut tabanlı rota optimizasyonu uygulaması	Rota talep bilgileri analiz uygulaması
Trafik Tıkanıklığı Bazlı Ücretlendirme	Rota-ücret optimizasyonu sezgisel algoritmalar kullanımı	Veri istatistik paylaşımı
Akıllı Toplu Taşıma Yönlendirme Sistemi	Rota-ücret optimizasyonu	Veri istatistik paylaşımı
Araç Paylaşımı	Rota-paydaş optimizasyonu	Veri istatistik paylaşımı
Bisiklet Paylaşımı	Rota-paydaş optimizasyonu	Veri istatistik paylaşımı
Çok Modlu Toplu Taşıma	Rota-arac-süre optimizasyonu	Veri istatistik paylaşımı

2.2 Akıllı Sağlık

Tanım : Akıllı sağlık, yaşam kalitesini artırmayı hedefleyen, sağlık hizmetlerini iyileştiren, bireylerin sağlıkları ile ilgili farkındalıklarını artıran, sağlık verisini akıllı bir şekilde analiz edilmesini sağlayan uygulama ve hizmetlerdir.(*AKILLI ŞEHİRLER – 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*, t.y.) Uygulama matrisi Çizelge 2’de verilmiştir.

Çizelge 2. Akıllı Sağlık Hesaplama Uygulamaları Matrisi.

Örnek Uygulama	Homomorfik Şifreleme	Güvenli Çok Taraflı Hesaplama
Mobil Sağlık Uygulamaları	Merkezi görüntü ve tahlile dayalı teşhis ve analiz	Giyilebilir sensör ve lokasyon verileri hesaplamaları
Giyilebilir Sağlık Teknolojileri	Merkezi görüntü ve tahlile dayalı teşhis ve analiz	Sensör verileri hesaplamaları
Uzaktan Hasta Takibi	Sağlıkta makine öğrenmesi uygulamaları	Hasta istatistikleri analizi ve federe öğrenme uygulamaları
Bireylerin Hastanelere Yönelmeden Önce Ayakta Tedavi Hizmetleri	Merkezi görüntü ve tahlile dayalı teşhis ve analiz	Hasta istatistikleri analizi ve federe öğrenme uygulamaları
Yaşlı, Kronik ve Engelli İçin Evde Hasta Desteği	Merkezi görüntü ve tahlile dayalı teşhis ve analiz	Hasta istatistikleri analizi ve federe öğrenme uygulamaları
Farkındalık Oluşturan Koruyucu Sağlık Hizmetleri	Merkezi görüntü ve tahlile dayalı teşhis ve analiz	Hasta istatistikleri analizi ve federe öğrenme uygulamaları
Kronik Hasta Takibi ve Panik Butonu Hizmeti	Merkezi görüntü ve tahlile dayalı teşhis ve analiz	Hasta istatistikleri analizi ve federe öğrenme uygulamaları

2.3 Akıllı Enerji

Tanım : Enerji ve kaynak açısından yüksek düzeyde verimli ve giderek artan bir şekilde yenilenebilir enerji kaynakları ile desteklenen, maliyet ve enerji tasarrufu sağlayan; stratejik planlama için entegre ve esnek kaynak sistemlerinin yanı sıra iç görüye dayalı, kamusal değeri olan ve yenilikçi yaklaşımlara dayanan şebekeler ile enerjinin yönetimidir.(*AKILLI ŞEHİRLER – 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*, t.y.) Uygulama matrisi Çizelge 3’de verilmiştir.

Çizelge 3. Akıllı Ulaşım Hesaplama Uygulamaları Matrisi.

Örnek Uygulama	Homomorfik Şifreleme	Güvenli Çok Taraflı Hesaplama
Akıllı Enerji Ağları ve Yönetimi	X	Tüketim ve üretim verileri analizleri
Enerji Depolama ve Yönetimi	Depolama planlaması ve optimizasyonu	Tüketim ve üretim verileri analizleri
Akıllı Enerji Üretimi ve Dağıtımı	Üretim planlaması	Tüketim ve üretim verileri analizleri
Akıllı Şebeke İstasyonları	Kestirimci bakım uygulamaları	X
Uzaktan Gözetim, İleri Kontrol Metotları ve Otomasyon (SCADA Sistemi)	Kestirimci bakım ve risk uygulamaları	X
Dağıtık Enerji Kaynakları ve Yönetimi	Dağıtık kaynak optimizasyonu	Tüketim ve üretim verileri analizleri
Akıllı Enerji İzleme Sistemleri	Kestirimci bakım ve risk uygulamaları	Tüketim ve üretim verileri analizleri

4. SONUÇ

Bu bildiride, akıllı şehir uygulamaları kapsamında şehir ekosistemi içerisinde üretilecek, transfer edilebilecek, işlenebilecek ve farklı uygulamalar içerisinde işlenebilecek veriler için güvenli veri işleme ve paylaşma altyapısına yönelik olarak güvenli çok taraflı hesaplama algoritmaları ve yine benzer şekilde güvenli veri işlenebilmesine imkan sağlayan homomorfik şifreleme uygulamalarına yönelik örnekler ve modeller sunulmaktadır. Yapılan çalışmalar için akıllı şehirler stratejileri ve eylem planında önceliklendirilmiş ve hali hazırda bazı illerde pilot uygulama veya yaygınlaştırma aşamasında olan uygulamalar ele alınmaya çalışılmıştır. Uygulamalar için ulaşım, sağlık ve enerji gibi verinin mahremiyeti ve verinin farklı yaklaşımlarda değerli bir varlık olarak ele alınabileceği çözümler tercih edilmiştir. Yapılan çalışma diğer uygulamalar için de benzer şekilde yaygınlaştırılabilir ve örnekler çoğaltılabilir. Özellikle büyük veri ve internet altyapısının yüksek hızlarda yaygınlaşıp bulut bilişim servislerinin de akıllı şehirler ekosisteminde daha etkin yer alması ile birlikte bu çalışmaların etkisinin artması düşünülmektedir.

KAYNAKLAR

- Aaltonen, A., Alaimo, C., & Kallinikos, J., 2021, The Making of Data Commodities: Data Analytics as an Embedded Process. *Journal of Management Information Systems*, 38(2, <https://doi.org/10.1080/07421222.2021.1912928>
- Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A., 2022, Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. İçinde *Computer Science Review*, C. 43, <https://doi.org/10.1016/j.cosrev.2021.100452>
- AKILLI ŞEHİRLER – 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı., t.y., Geliş tarihi 24 Ekim 2022, gönderen <https://www.akillisehirler.gov.tr/>
- al Nuaimi, E., al Neyadi, H., Mohamed, N., & Al-Jaroodi, J., 2015, Applications of big data to smart cities. *Journal of Internet Services and Applications*, 6(1, <https://doi.org/10.1186/s13174-015-0041-5>
- Alexei, A., & Alexei, A., 2021, Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific & Technology Research*, 10(3,
- Alizadeh, F., Jakobi, T., Boldt, J., & Stevens, G., 2019, GDPR-reality check on the right to access data. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3340764.3344913>
- Allam, Z., & Dhunny, Z. A., 2019, On big data, artificial intelligence and smart cities. *Cities*, 89. <https://doi.org/10.1016/j.cities.2019.01.032>
- Anthony, B., Petersen, S. A., & Helfert, M., 2020, Digital Transformation of Virtual Enterprises for Providing Collaborative Services in Smart Cities. *IFIP Advances in Information and Communication Technology*, 598. https://doi.org/10.1007/978-3-030-62412-5_21
- Barnett, J. H., 2009, Early writings on graph theory: Topological connections. İçinde *Resources for Teaching Discrete Mathematics: Classroom Projects, History Modules, and Articles*. <https://doi.org/10.5948/UPO9780883859742.030>
- BAYGÜL ÖZPINAR, Ş., & ÖZPINAR, A., 2021, Halkla İlişkiler Ajansları için Bulut Tabanlı Güvenli Çok Taraflı Hesaplama ve İşbirliği Servisi - SMPCCaaS. *European Journal of Science and Technology*. <https://doi.org/10.31590/ejosat.1013962>
- BenaissáBenaissá Ecole Supérieure en Informatique, A., Bel Abbès, S., Algeria, O., Cebere OpenMined, B., & Eddine BelfedhaiBelfedhai, A., 2021, *TenSEAL: A Library for Encrypted Tensor Operations Using Homomorphic Encryption*. <https://doi.org/10.48550/arxiv.2104.03152>
- Bethencourt, J., Sahai, A., & Waters, B., 2007, Ciphertext-policy attribute-based encryption. *Proceedings - IEEE Symposium on Security and Privacy*. <https://doi.org/10.1109/SP.2007.11>
- Bibri, S. E., 2018, The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. *Sustainable Cities and Society*, 38. <https://doi.org/10.1016/j.scs.2017.12.034>
- Birch, K., Cochrane, D. T., & Ward, C., 2021, Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. *Big Data and Society*, 8(1, <https://doi.org/10.1177/20539517211017308>
- Caragliu, A., del Bo, C., & Nijkamp, P., 2011, Smart cities in Europe. *Journal of Urban Technology*, 18(2), 65-82. <https://doi.org/10.1080/10630732.2011.601117>
- Chen, D., Doumeingts, G., & Vernadat, F., 2008, Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry*, 59(7, <https://doi.org/10.1016/j.compind.2007.12.016>
- Chen, H., Laine, K., & Player, R., 2017, Simple encrypted arithmetic library - SEAL v2.1. *Lecture Notes in Computer Science, Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 10323 LNCS. https://doi.org/10.1007/978-3-319-70278-0_1
- Cheon, J. H., Kim, D., Kim, D., Lee, H. H., & Lee, K., 2019, Numerical Method for Comparison on Homomorphically Encrypted Numbers. *Lecture Notes in Computer Science, Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 11922 LNCS. https://doi.org/10.1007/978-3-030-34621-8_15
- Cheon, J. H., Kim, D., Kim, Y., & Song, Y., 2018, Ensemble method for privacy-preserving logistic regression based on homomorphic encryption. *IEEE Access*, 6. <https://doi.org/10.1109/ACCESS.2018.2866697>
- Chung, L., & Subramanian, N., 2007, Bridging the gap between enterprise architectures and software architectures. İçinde *Science of Computer Programming*, C. 66, Issue 1, <https://doi.org/10.1016/j.scico.2006.12.001>
- Clastres, C., 2011, Smart grids: Another step towards competition, energy security and climate change objectives. *Energy Policy*, 39(9, <https://doi.org/10.1016/j.enpol.2011.05.024>
- Cui, Y., Li, S., Wang, Y., & Gao, B., 2020, The data protection of intelligent connected vehicles cloud control framework using fully homomorphic encryption. 2020 4th CAA International Conference on Vehicular Control and Intelligence, CVCi 2020. <https://doi.org/10.1109/CVCi51460.2020.9338620>
- Damgård, I., Pastro, V., Smart, N., & Zakarias, S., 2012, Multiparty computation from somewhat homomorphic encryption. *Lecture Notes in Computer Science, Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 7417 LNCS. https://doi.org/10.1007/978-3-642-32009-5_38
- Ding, D., Chong, G., Lee Kuo Chuen, D., & Cheng, T. L., 2018, From Ant Financial to Alibaba's Rural Taobao Strategy - How Fintech Is Transforming Social Inclusion. İçinde *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation*. <https://doi.org/10.1016/B978-0-12-810441-5.00002-6>

- Fan, J., & Vercauteren, F., 2012, Somewhat Practical Fully Homomorphic Encryption. *Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography*.
- Farokhi, F., Shames, I., & Johansson, K. H., 2020, Private routing and ride-sharing using homomorphic encryption. *IET Cyber-Physical Systems: Theory and Applications*, 5(4), 311-320. <https://doi.org/10.1049/IET-CPS.2019.0042>
- Gautier, A., & Lamesch, J., 2021, Mergers in the digital economy. *Information Economics and Policy*, 54. <https://doi.org/10.1016/j.infoecopol.2020.100890>
- Giannotti, F., Nanni, M., Pinelli, F., & Pedreschi, D., 2007, Trajectory pattern mining. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. <https://doi.org/10.1145/1281192.1281230>
- GitHub - OpenMined/SyMPC: A SMPC companion library for Syft., t.y., Geliş tarihi 24 Ekim 2022, gönderen <https://github.com/OpenMined/SyMPC>
- Global Data Thematic Research., 2020, History of smart cities: Timeline. İçinde *Verdict.co.uk*.
- Goyal, V., Pandey, O., Sahai, A., & Waters, B., 2006, Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the ACM Conference on Computer and Communications Security*. <https://doi.org/10.1145/1180405.1180418>
- Gupta, S., Chen, H., Hazen, B. T., Kaur, S., & Santibañez Gonzalez, E. D. R., 2019, Circular economy and big data analytics: A stakeholder perspective. *Technological Forecasting and Social Change*, 144. <https://doi.org/10.1016/j.techfore.2018.06.030>
- Hajjaji, Y., Boulila, W., Farah, I. R., Romdhani, I., & Hussain, A., 2021, Big data and IoT-based applications in smart environments: A systematic review. İçinde *Computer Science Review*, C. 39, <https://doi.org/10.1016/j.cosrev.2020.100318>
- Halevi, S., & Shoup, V., 2014, Algorithms in HELib. *Lecture Notes in Computer Science, Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 8616 LNCS(PART 1, https://doi.org/10.1007/978-3-662-44371-2_31
- Halevi, S., & Shoup, V., 2020, Design and implementation of HELib : a homomorphic encryption library. *EPrint*, 1481(Report 2020/1481,
- Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., & Chiroma, H., 2016, The role of big data in smart city. *International Journal of Information Management*, 36(5, <https://doi.org/10.1016/j.ijinfomgt.2016.05.002>
- Hina, S., & Dominic, P. D. D., 2020, Information security policies' compliance: a perspective for higher education institutions. İçinde *Journal of Computer Information Systems*, C. 60, Issue 3, <https://doi.org/10.1080/08874417.2018.1432996>
- Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S., 2015, The internet of things for health care: A comprehensive survey. *IEEE Access*, 3. <https://doi.org/10.1109/ACCESS.2015.2437951>
- Jacobson, M. Z., 2009, Review of solutions to global warming, air pollution, and energy security. İçinde *Energy and Environmental Science*, C. 2, Issue 2, <https://doi.org/10.1039/b809990c>
- Javornik, M., Nadoh, N., & Lange, D., 2019, *Data Is the New Oil*. https://doi.org/10.1007/978-3-319-99756-8_19
- Jiang, H., Liu, Y., Song, X., Wang, H., Zheng, Z., & Xu, Q., 2020, Cryptographic Approaches for Privacy-Preserving Machine Learning. *Dianzi Yu Xinxu Xuebao/Journal of Electronics and Information Technology*, 42(5), 1068-1078. <https://doi.org/10.11999/JEIT190887>
- Kim, J. H., 2022, Smart city trends: A focus on 5 countries and 15 companies. *Cities*, 123. <https://doi.org/10.1016/j.cities.2021.103551>
- Laidroo, L., & Avarmaa, M., 2020, The role of location in FinTech formation. *Entrepreneurship and Regional Development*, 32(7-8, <https://doi.org/10.1080/08985626.2019.1675777>
- Lamport, L., 1981, Password Authentication with Insecure Communication. *Communications of the ACM*, 24(11, <https://doi.org/10.1145/358790.358797>
- Lemus, M., Ramos, M. F., Yadav, P., Silva, N. A., Muga, N. J., Souto, A., Paunković, N., Mateus, P., & Pinto, A. N., 2020, Generation and Distribution of Quantum Oblivious Keys for Secure Multiparty Computation. *Applied Sciences* 2020, Vol. 10, Page 4080, 10(12), 4080. <https://doi.org/10.3390/APP10124080>
- Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W., 2013, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, 24(1, <https://doi.org/10.1109/TPDS.2012.97>
- Lin, C., Li, G., Shan, Z., & Shi, Y., 2017, Thinking and modeling for big data from the perspective of the I Ching. *International Journal of Information Technology and Decision Making*, 16(6, <https://doi.org/10.1142/S0219622017500286>
- Mazzi, F., Adonis, A., Cows, J., Tsamados, A., Taddeo, M., & Floridi, L., 2021, The UK GDPR Reform: missing data privacy, regulatory probity, and harm prevention. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3974832>
- Meel, P., & Vishwakarma, D. K., 2020, Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. İçinde *Expert Systems with Applications*, C. 153, <https://doi.org/10.1016/j.eswa.2019.112986>

- Munjal, K., & Bhatia, R., 2022, A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex and Intelligent Systems*, 1-28. <https://doi.org/10.1007/S40747-022-00756-Z/TABLES/6>
- Needham, R. M., & Schroeder, M. D., 1978, Using Encryption for Authentication in Large Networks of Computers. *Communications of the ACM*, 21(12), <https://doi.org/10.1145/359657.359659>
- Ni, J., Zhang, K., Lin, X., & Shen, X. S., 2018, Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. *IEEE Communications Surveys and Tutorials*, 20(1), <https://doi.org/10.1109/COMST.2017.2762345>
- Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M., 2021, Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. *Evolving Systems*, 12(1), <https://doi.org/10.1007/s12530-020-09335-4>
- Rausand, M., & Haugen, S., 2020, Risk assessment: Theory, methods, and applications. İçinde *Risk Assessment: Theory, Methods, and Applications*. <https://doi.org/10.1002/9781119377351>
- Richter, H., & Slowinski, P. R., 2019, The Data Sharing Economy: On the Emergence of New Intermediaries. *IIC International Review of Intellectual Property and Competition Law*, 50(1), <https://doi.org/10.1007/s40319-018-00777-7>
- Rivest, R. L., Shamir, A., & Tauman, Y., 2001, How to leak a secret. *Lecture Notes in Computer Science, Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 2248. https://doi.org/10.1007/3-540-45682-1_32
- Saha, D., Young, T., & Thacker, J., 2021, Data privacy and competition law at the crossroads. İçinde *Economic and Political Weekly*, C. 56, Issue 39,
- Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A., 2011, Smart cities and the future internet: Towards cooperation frameworks for open innovation. *Lecture Notes in Computer Science, Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 6656. https://doi.org/10.1007/978-3-642-20898-0_31
- Shamir, A., 1979, How to Share a Secret. *Communications of the ACM*, 22(11), <https://doi.org/10.1145/359168.359176>
- Shamir, A., Rivest, R. L., & Adleman, L. M., 1981, Mental Poker. İçinde *The Mathematical Gardner*. https://doi.org/10.1007/978-1-4684-6686-7_5
- Shu, H., 2016, Big data analytics: six techniques. *Geo-Spatial Information Science*, 19(2), <https://doi.org/10.1080/10095020.2016.1182307>
- Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J., 2019, Cyber risk and insurance for transportation infrastructure. *Transport Policy*, 79. <https://doi.org/10.1016/j.tranpol.2019.04.019>
- Ulven, J. B., & Wangen, G., 2021, A systematic review of cybersecurity risks in higher education. İçinde *Future Internet*, C. 13, Issue 2, <https://doi.org/10.3390/fi13020039>
- Usman, M., Asghar, M. R., Ansari, I. S., Granelli, F., & Qaraqe, K. A., 2018, Technologies and Solutions for Location-Based Services in Smart Cities: Past, Present, and Future. *IEEE Access*, 6. <https://doi.org/10.1109/ACCESS.2018.2826041>
- van den Buuse, D., & Kolk, A., 2019, An exploration of smart city approaches by international ICT firms. *Technological Forecasting and Social Change*, 142, 220-234. <https://doi.org/10.1016/j.techfore.2018.07.029>
- Voorwinden, A., 2021, The privatised city: technology and public-private partnerships in the smart city. *Law, Innovation and Technology*, 13(2), <https://doi.org/10.1080/17579961.2021.1977213>
- Wang, D., & Zhang, X., 2020, Secure data sharing and customized services for intelligent transportation based on a consortium blockchain. *IEEE Access*, 8. <https://doi.org/10.1109/ACCESS.2020.2981945>
- Yao, A. C., 1982a, PROTOCOLS FOR SECURE COMPUTATIONS. *Annual Symposium on Foundations of Computer Science - Proceedings*. <https://doi.org/10.1109/sfcs.1982.38>
- Yao, A. C., 1982b, PROTOCOLS FOR SECURE COMPUTATIONS. *Annual Symposium on Foundations of Computer Science - Proceedings*, 160-164. <https://doi.org/10.1109/sfcs.1982.38>
- Yao, A. C. C., 1986, HOW TO GENERATE AND EXCHANGE SECRETS. *Annual Symposium on Foundations of Computer Science, Proceedings*, <https://doi.org/10.1109/sfcs.1986.25>
- Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C. Z., Li, H., & Tan, Y. an., 2019, Secure Multi-Party Computation: Theory, practice and applications. *Information Sciences*, 476, 357-372. <https://doi.org/10.1016/j.ins.2018.10.024>
- Ziller, A., Trask, A., Lopardo, A., Szymkow, B., Wagner, B., Bluemke, E., Nounahon, J. M., Passerat-Palmbach, J., Prakash, K., Rose, N., Ryffel, T., Reza, Z. N., & Kaissis, G., 2021, PySyft: A Library for Easy Federated Learning. *Studies in Computational Intelligence*, 965, 111-139. https://doi.org/10.1007/978-3-030-70604-3_5/COVER