Derleme Makalesi

NESNELERİN İNTERNETİNDE VERİ MAHREMİYETİNİN KORUNMASI ÜZERİNE BİR İNCELEME

Murat Utku KABASAKALOĞLU, Can EYÜPOĞLU
Milli Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye
utkukabasakal58@gmail.com, caneyupoglu@gmail.com
0009-0009-7047-7764, 0000-0002-6133-8617

Atıf/Citation: Kabasakaloğlu M. U., Eyüpoğlu C., (2025), NESNELERİN İNTERNETİNDE VERİ MAHREMİYETİNİN KORUNMASI ÜZERİNE BİR İNCELEME, İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi, Cilt 8, No 1, s. 143-xx, DOI: 10.56809/icujtas.1630096

ÖZET

Nesnelerin İnterneti (Internet of Things-IoT) ve büyük veri teknolojileri, karmaşık analitik ve karar verme prosedürlerini kolaylaştırarak çok sayıda sektörü dönüştürmüştür. Bununla birlikte, IoT cihazlarının topladığı büyük miktarda hassas veri nedeniyle önemli gizlilik ve güvenlik endişeleri ortaya çıkmıştır. Bu çalışmada, büyük veri ve IoT senaryolarında uygulanan gizlilik koruma stratejilerinin kapsamlı bir literatür değerlendirmesi sunulmaktadır. Gizlilik mühendisliği metodolojileri, IoT'ye özgü gizlilik koruma önlemleri, anonimleştirme teknikleri ve diferansiyel gizlilik stratejileri tartışılmaktadır. Sonuçlar, diferansiyel gizlilik ve homomorfik şifreleme gibi tekniklerin büyük veri ve IoT ortamlarında gizliliği iyileştirmek için iyi çalıştığını göstermektedir. Ayrıca, anonimleştirme tekniklerinin sağlık ve endüstriyel IoT gibi sektörlerde veri mahremiyetini korumak için kullanılabileceği görülmüştür.

Anahtar Kelimeler: Nesnelerin İnterneti, Büyük Veri, Veri Mahremiyeti, Anonimleştirme Teknikleri, Diferansiyel Gizlilik, Gizlilik Mühendisliği

A REVIEW ON DATA PRIVACY PRESERVATION IN INTERNET OF THINGS

ABSTRACT

The Internet of Things (IoT) and big data technologies have transformed numerous industries by streamlining complex analytics and decision-making procedures. On the other hand, significant privacy and security concerns have emerged due to the large amount of sensitive data collected by IoT devices. This study presents a comprehensive literature review of privacy preservation strategies applied in big data and IoT scenarios. Privacy engineering methodologies, IoT-specific privacy protection measures, anonymization techniques, and differential privacy strategies are discussed. The results show that techniques such as differential privacy and homomorphic encryption work well for improving privacy in big data and IoT environments. Furthermore, anonymization techniques can be used to protect data privacy in sectors such as healthcare and industrial IoT.

Keywords: Internet of Things, Big Data, Data Privacy, Anonymization Techniques, Differential Privacy, Privacy Engineering

Geliş/Received	**:**	**30.01.2025**
Gözden Geçirme/Revised	**:**	**01.09.2025**
Kabul/Accepted	**:**	**09.03.2025**

1. GİRİŞ

Büyük veri ve Nesnelerin İnterneti (Internet of Things-IoT) teknolojilerinin yaygın kullanımı topluma büyük fayda sağlamaktadır. Ancak bu teknolojilerin kullanılması ile birlikte gizlilik ve güvenlik endişeleri de ortaya çıkmaktadır. Çeşitli alanlardaki karar alma süreçleri, IoT cihazları tarafından toplanan verilerin sürekli artan hacmi ve çeşitliliğinin analizi ile desteklenmektedir. Bununla birlikte, toplanan verilerin hassas ve gizli doğası nedeniyle insanların mahremiyetinin korunması ihtiyacı oluşmaktadır (Du ve ark., 2018; Yang ve ark., 2016).

IoT ortamlarıyla ilgili temel sorunlardan biri, IoT cihazlarının genellikle düşük işlem ve enerji kapasitelerine sahip olmasıdır. Bu nedenlerle de geleneksel güvenlik teknikleri yetersiz kalmaktadır ve IoT cihazlarına özgü güvenlik ve gizlilik prosedürlerinin geliştirilmesi gerekmektedir. Örneğin, veriler homomorfik şifreleme teknikleri kullanılarak şifrelenmiş biçimde işlenebilir. IoT cihazlarının kısıtlı kaynakları göz önünde bulundurulduğunda, homomorfik şifreleme verilerin şifrelenmiş biçimde işlenmesini sağlar. Ayrıca, büyük veri analitiği sırasında, diferansiyel gizlilik (differential privacy) tabanlı teknikler kişisel bilgilerin gizliliğini korurken analizin doğruluğunu sağlamaktadır (Kara ve Eyüpoğlu, 2020; Seliem ve ark., 2018). Literatürdeki araştırmalara göre bireylerin özel bilgilerini gizli tutmak için *l*-çeşitlilik, *t*-yakınlık ve *k*-anonimlik gibi teknikler sıklıkla kullanılmaktadır (Kara ve Eyüpoğlu, 2023). Özellikle sağlık sektöründeki hasta verilerinin korunmasında anonimleştirme stratejilerinden oldukça faydalanılmaktadır (Eyüpoğlu ve ark., 2017; Eyüpoğlu, 2018; Xu ve ark., 2014).

Sürekli veri akışı ve IoT cihazlarının heterojen mimarisi, bu cihazlardan toplanan verilerin güvenliğini daha da zorlaştırmaktadır. Yang ve ark. (2016), çoklu bulut ortamında IoT cihazlarından gelen verileri güvenli bir şekilde paylaşmak için bir model geliştirmiştir. Bu model, veri paylaşımında hem gizliliği hem de doğruluğu artırmak için şifreleme ve anonimleştirme tekniklerini birleştirmektedir. Benzer şekilde, Jiang ve ark. (2021) tarafından yapılan çalışma, farklı gizlilik stratejilerinin yalnızca endüstriyel IoT uygulamalarında bireysel gizliliği korumakla kalmayıp aynı zamanda operasyonel verimliliği de yukarıya çıkarabileceğini göstermektedir.

Büyük veri ve IoT tabanlı verilerin kullanıldığı durumlarda, gizliliğin korunması güvenliğin temeli olarak görülmektedir. Veri işlerken gizliliği sağlamanın başlıca yolları; anonimleştirme, diferansiyel gizlilik, çoklu bulut tabanlı şifreleme ve dağıtık veri gizliliği teknikleri gibi teknolojilerdir. Bununla birlikte, bu yöntemlerin artan veri, yoğun talepler ve tehditler karşısında uygulanabilir ve başarılı olup olmadığı hala tartışılmaktadır (Eyüpoğlu ve ark., 2017; Gümüş ve Eyüpoğlu, 2022).

Bu çalışmada, büyük veri ve IoT ortamlarında gizliliği koruma teknikleri üzerine bir literatür taraması sunulmaktadır. Mevcut yaklaşımların sınıflandırılmasından, performanslarının değerlendirilmesinden ve uygulama alanlarındaki etkinliklerinin incelenmesinden bahsedilmektedir. Ayrıca, IoT uygulamaları için oluşturulan yeni yöntemler ve bunların güvenlik üzerindeki etkileri kapsamlı bir şekilde incelenmektedir. Verilerin güvenli bir şekilde paylaşılmasına yönelik dağıtık mimariler ve uç bilişim teknikleri gibi yeni çözümler de araştırmanın öne çıkan konularından biri olarak değerlendirilmektedir. Bu bağlamda çalışma, yalnızca mevcut yaklaşımların etkinliğini değerlendirmeyi değil, aynı zamanda IoT ve büyük veri ortamlarında karşılaşılan mevcut zorluklara ve gelecekteki yönlere ışık tutmayı da amaçlamaktadır.

Çalışmanın geri kalanı şu şekilde organize edilmiştir: 2. Bölümde anonimleştirme teknikleri ve uygulamaları, diferansiyel gizlilik yaklaşımları, IoT uygulamalarında gizlilik koruma ve güvenlik, büyük veride güvenlik ve mahremiyet ve mahremiyet mühendisliği yaklaşımları konularında gerçekleştirilen literatür taramasına yer verilmektedir. 3. Bölümde literatürdeki çalışmalar bir tablo halinde karşılaştırılmaktadır. Son olarak 4. Bölümde ise çalışmanın genel sonuçlarına değinilmektedir.

2. LİTERATÜR TARAMASI

2.1. Anonimleştirme Teknikleri ve Uygulamaları

Gizliliğin korunmasına yönelik en önemli tekniklerden biri, kişilerin kimliklerini açıklamadan veri alışverişinde bulunmalarına olanak tanıyan anonimleştirmedir (Eyupoglu ve ark., 2018). Kişisel bilgilerin ifşa edilmeden veri paylaşımına olanak sağlayan temel bir mekanizma olan anonimleştirme, büyük veri ve IoT ortamlarında gizliliğin korunması açısından çok büyük öneme sahiptir. Bu tekniklerin uygulanması, IoT cihazlarından gelen büyük miktarlardaki veriler işlenirken, veri analitiği faaliyetlerinin sürekliliğini ve yasal gerekliliklere uygunluğu sağlamak için önemlidir. Ancak IoT cihazlarının sınırlı işlem gücü ve veri hareketliliği gibi özellikleri, kayıt

yöntemlerinin uygulanmasında benzersiz zorluklar ortaya çıkarmaktadır. Literatürde kayıt yöntemleri, genellikle veri azaltma, saldırı direnci ve gizlilik ödünleşimlerine odaklanmaktadır.
k-anonimlik, *l*-çeşitlilik, *t*-yakınlık gibi teknikler büyük veri setlerinde bireysel kimliklerin açığa çıkmasını engellemek için sıklıkla tercih edilen yöntemlerdir. *k*-anonimlik, bir veri kümesindeki her bireyin en az "*k*" bireyle aynı özelliklere sahip olmasını sağlayarak gizliliği korumaktadır. Tıp alanında yaygın olarak kullanılan bu yöntem, hasta verilerinin anonim olarak paylaşılmasına yönelik güçlü bir araç olarak öne çıkmaktadır. Öte yandan *k*-anonimleştirme, yüksek boyutlu verilere uygulandığında arama girişimlerine karşı yeterli koruma sağlayamayabilmektedir (Kara ve Eyüpoğlu, 2020, 2021; Kara ve ark., 2023).

IoT ortamlarındaki cihazların ve verilerin dinamik doğası nedeniyle kayıt çözümleri daha karmaşık hale gelmiştir. Literatürdeki bazı çalışmalar, *k*-anonimlik ve *t*-yakınlık yöntemlerinin sağlık alanındaki etkinliğini araştırmış ve büyük ölçekli saldırılara karşı dayanıklılığı artırdıkları sonucuna varmışlardır. Benzer şekilde Seliem ve ark. (2018), IoT verilerinin korunmasına yönelik var olan uygulamaları incelemiş ve bu uygulamalardaki güvenlik ile gizlilik arasındaki dengenin önemini vurgulamıştır.

Gümüş ve Eyüpoğlu (2022) tarafından yapılan çalışmada büyük veri analitiğinde kullanılan anonimleştirme teknikleri araştırılmış, büyük veriler üzerinde gerçekleştirilebilecek saldırı teknikleri açıklanmış ve kişi mahremiyetinin nasıl sağlanacağı konusu üzerinde durulmuştur. Uluç ve Eyüpoğlu (2024) ise çalışmalarında IoT cihazı olarak kullanılan akıllı saatlerde meydana gelebilecek mahremiyet ve güvenlik problemlerini incelemiştir.

Kimliği korurken veriler üzerinde hareket edebilme, uyumluluğu sağlama ve güvenli veri paylaşımını kolaylaştırma, anonimleştirme yaklaşımlarının faydalarından bazılarıdır. Ancak bu yöntemlerin sınırlamalarını dikkate almak önemlidir. Bazı teknikler yeniden tanımlama girişimlerine karşı yeterli koruma sağlayamamakta ve özellikle yüksek boyutlu veri setlerinde bilgi kaybı yaşanabilmektedir (Yang ve ark., 2016).

Ahmetoğlu ve Daş (2022), IoT cihazlarından elde edilen büyük verilerin anonimleştirilmesi sırasında karşılaşılan sorunları analiz ederek *k*-anonimlik ve *t*-yakınlık gibi yöntemlerinin avantaj ve dezavantajlarını araştırmışlardır. Çalışmada, veri türlerini korurken kayıt yöntemlerinin saldırı direncini artırmayı amaçlayan stratejiler ve IoT ortamlarında anonimleştirme tekniklerinin geliştirilmesine yönelik yeni öneriler sunulmaktadır.

Perera ve ark. (2015), IoT alanında anonimleştirme tekniklerinin uygulanmasını incelemiş ve büyük verinin mahremiyetini korumanın yollarını tartışmışlardır. IoT cihazlarından veri kimlik doğrulaması için mevcut anonimleştirme yöntemleri incelenmiştir. Ayrıca, IoT bağlamında karşılaşılan benzersiz zorlukların üstesinden gelmek için bu stratejilerin nasıl değiştirilebileceğine dair öneriler de sunulmaktadır. IoT cihazlarının ihtiyaçlarına göre uyarlanmış kayıt yöntemlerinin geliştirilmesiyle literatürü katkı sağlanmıştır.

Yapay zeka entegrasyonuna sahip IoT tabanlı bulut sistemlerinde veri gizliliğinin korunmasına yönelik anonimleştirme teknikleri Dhinakaran ve ark. (2024) tarafından tartışılmıştır. IoT cihazlarından veri kodlamaya yönelik geleneksel yaklaşımların yanı sıra yapay zeka tarafından desteklenen potansiyel yaklaşımlar da araştırılmıştır. Özellikle diferansiyel gizlilik ve homomorfik şifreleme gibi tekniklerin IoT cihazları için uygunluğu incelenmiştir. Bu çalışmanın, literatüre anonimleştirme yöntemlerini optimize etmek için yapay zekanın kullanımına ilişkin yenilik kattığı değerlendirilmektedir.

Anonimleştirme tekniklerinin büyük verilere uygulanmasına ilişkin kapsamlı bir inceleme Binjubeir ve ark. (2019) tarafından yapılmıştır. Çalışmada literatürde var olan sorunlar için önerilen çözümler ve IoT cihazlarından anonim olarak veri toplanmasında karşılaşılan zorluklar araştırılmıştır. Çalışma ile büyük veri sistemlerinde anonimleştirme tekniklerinin geliştirilmesine yönelik bir metodoloji kılavuzu sağlanmıştır.

Bu bölümde literatürdeki çalışmalar analiz edilmiş ve IoT'de kayıt yöntemlerinin uygulanmasına yönelik yaklaşımlar anlatılmıştır. Yapılan incelemeye göre kayıt mekanizmalarının, büyük veri ve IoT politikalarındaki gizlilik kaygılarını çözebileceği değerlendirilmektedir. Özetle, anonimleştirme teknikleri büyük veri ve IoT ortamlarında gizliliğin korunması için önemli bir araç olarak düşünülmektedir. Ancak İnternet'in tutarlı verileri ve güçlü manipülasyonu gibi özellikleri nedeniyle bu tekniklerin karmaşık, esnek ve ölçeklenebilir bir şekilde uygulanması gerekmektedir. Bu durumda kayıt prosedürlerinin etkinliğini daha da artırmak için yeni yöntemler geliştirilmelidir.

2.2. Diferansiyel Gizlilik Yaklaşımları

Diferansiyel gizlilik, özellikle büyük veri ve IoT bağlamında veri gizliliğini koruma yöntemleri arasında önemli bir yere sahiptir. Bu yaklaşım, veriler üzerinde yapılan analizlerin sonuçlarını etkilemeden, bireylerin gizliliğini

garanti altına almayı hedeflemektedir. Literatürde, diferansiyel gizlilik yöntemleri, genellikle veri setlerindeki hassas bilgilerin ifşa edilmesini önlemek için kullanılan matematiksel çerçevelerle uygulanmaktadır. Bu bölümde, bu tekniklerin IoT ve büyük veri ortamlarındaki uygulamaları ve literatüre sağladığı katkılar incelenmektedir.

IoT cihazlarından toplanan verilere güvenli ve gizlilik odaklı bir yaklaşımın uygulanması, olası veri ihlallerinin önlenmesine yardımcı olmaktadır ve özellikle iş dünyasında üretim ve enerjide kullanılabilirliği artırmaktadır. IoT'de veri güvenliğini artırmada farklı gizlilik stratejilerinin rolü Perera ve ark. (2015) tarafından tartışılmıştır. Çalışmada, IoT cihazlarından toplanan farklı veri setlerinin, farklı gizlilik korumalarını uygulamak için nasıl kullanılabileceği tartışılmıştır. Farklı gizlilik stratejileri için gerçek dünyadaki kullanım örnekleri analiz edilmiş ve özel verilerin IoT cihazlarından en iyi şekilde nasıl korunduğu araştırılmıştır. Bu çalışma, IoT cihaz veri gizliliğini geliştirmek için gizlilik farklılıklarının kullanımına ilişkin araştırmalara önemli ölçüde katkıda bulunmuştur.

Dhinakaran ve ark. (2024), IoT tabanlı bulut sistemlerindeki farklı gizlilik stratejilerini yapay zeka ile birleştirerek tartışmıştır. Çalışmada, farklı gizlilik seviyelerinin IoT cihazlarından toplanan veri kümelerini saldırılara karşı nasıl daha dirençli hale getirebileceği incelenmiştir. Yapay zeka tarafından desteklenen farklı gizlilik stratejileri ile veri analizi doğruluğunun nasıl korunabileceği araştırılmıştır. Çalışmanın, IoT cihazlarında yapay zeka entegrasyonu ile diferansiyel gizlilik uygulamalarının optimizasyonuna ilişkin literatüre yeni bir bakış açısı sağladığı değerlendirilmektedir.

2.3. IoT Uygulamalarında Gizlilik Koruma ve Güvenlik

IoT uygulamaları günlük hayatın birçok alanında giderek yaygınlaşmaktadır, ancak gizlilik ve güvenlik endişeleri bu cihazların veri toplama, analiz etme ve paylaşma şeklinden kaynaklanmaktadır. Kalıcı veriler ve bilgisayar tarafından öğrenilebilir cihazlar, IoT ortamlarındaki güvenlik endişelerini daha da karmaşık hale getirmektedir. IoT cihazlarının yarattığı riskleri azaltmak için gizliliğin korunması ve güvenlik önlemleri konusunda literatürde çeşitli çalışmalar vardır. Bu bölümde IoT bağlamında güvenlik ve gizlilik stratejileri incelenmektedir.

Du ve ark. (2018), IoT cihazlarından oluşan Çoklu Erişimli Uç Bilişim (Multi-Access Edge Computing-MEC) ortamlarında büyük veri gizliliğini korumaya yönelik stratejileri tartışmıştır. Çalışmada, gizlilik ve homomorfik şifrelemenin MEC ortamlarında veri güvenliğini ve enerji verimliliğini nasıl etkilediği incelemektedir. Nihai ürüne yönelik veri toplama, işleme ve paylaşma prosedürleri sırasında ortaya çıkan güvenlik riskleri, olası çözümlerle birlikte irdelenmektedir. IoT cihazlarının gizlilik gereksinimlerini karşılamak için MEC bağlamlarında kullanılabilecek yaratıcı çözümler sunulmuştur.

Yang ve ark. (2016), IoT'de gizliliği koruyan çoklu bulut tabanlı bir veri yayınlama sistemi önermişlerdir. Çalışmada, şifreleme ve veri anonimleştirme tekniklerini birleştiren sistemlerinin kullanıcıları korurken veri analizinin doğruluğunu nasıl artırdığı açıklanmaktadır. Özellikle IoT cihazlarının çoklu bulut ortamlarında veri alışverişi yaparken karşılaştığı güvenlik kusurlarını ele almak amaçlanmaktadır. Çalışmada, çoklu bulut tabanlı IoT veri yönetimi için uygulanabilir bir yaklaşım sunulmuştur.

Polat ve ark. (2017), IoT uygulamalarında bölümlere ayrılmış verilere dayalı gizlilik koruma stratejilerini ele almıştır. Çalışmada, IoT cihazlarından elde edilen hassas verilerin şifrelenmesi ve verimli bir şekilde paylaşılması için veri segmentasyonu ve anonimleştirme teknikleri önerilmiştir. Gizlilik sızıntılarını önlemek için hibrit güvenlik önlemlerini analiz edilmiştir. Çalışmada, IoT cihazlarından elde edilen verilerin güvenliğini sağlamak için yeni yöntemler sunulmuştur.

Bu bölümde IoT uygulamalarında gizliliğin korunması ve güvenliğine yönelik çalışmalar anlatılmaktadır. Çalışmalarda, IoT cihazlarının sınırlı işlem gücü ve sürekli veri aktarımı gibi problemleri dikkate alınarak gizlilik ve güvenlik tehditlerini azaltmanın yeni yolları araştırılmaktadır.

2.4. Büyük Veride Güvenlik ve Mahremiyet

Bilginin hacmi ve çeşitliliği hızla arttıkça modern bilgi çağının en önemli özelliklerinden biri olarak büyük veri ortaya çıkmıştır. Veriler; gizlilik, veri güvenliği ve veri uygulamalarıyla ilgili riskler de dahil olmak üzere çok çeşitli riskler oluştururlar. Büyük veri araştırmalarında veri güvenliğinin sağlanması ve bireysel mahremiyetin korunması artık araştırmacılar tarafından oldukça önemsenmektedir.

Xu ve ark. (2014) tarafından gerçekleştirilen çalışmada, veri madenciliği teknikleri ve büyük verilerdeki gizlilik ve bilgi güvenliği endişeleri araştırılmıştır. Çalışmada büyük veri uygulamalarındaki güvenlik riskleri

sınıflandırılmış ve karşı önlemler tartışılmıştır. Özellikle, önerilen geçiş ve şifreleme yöntemlerinin hassas veri sızıntılarını önlemedeki etkinliği değerlendirilmiştir. Büyük veri bağlamında gizlilik ve güvenlik konuları kapsamlı bir şekilde incelenmiştir.

Wang ve ark. (2018) büyük veri analizinde IoT cihazlarından elde edilen verilerin gizliliğini ve güvenliğini tartışmışlardır. Çalışmada, gizlilik koruma stratejilerinin büyük veri ortamında nasıl uygulanabileceği araştırılmış ve sürekli veri aktarımı için IoT cihazlarının oluşturduğu güvenlik açıklarının kapatılmasına yönelik öneriler sunulmuştur.

Büyük veriye yönelik gizlilik ve güvenliğin korunmasına yönelik çalışmalar bu bölümde incelenmiştir. Çalışmalar, büyük veri analizinin ortaya çıkardığı zorlukları ele alırken güvenlik ve gizlilik koruma önlemlerini iyileştirmeye yönelik bir dizi öneri sunmaktadırlar.

2.5. Mahremiyet Mühendisliği Yaklaşımları

Gizlilik teknolojisi, gizlilik ihtiyaçlarını sistem tasarımına entegre ederek bireysel gizliliği korumanın bir yoludur. Bu alan, büyük veri platformları ve IoT cihazları için gizlilik tehditlerine karşı sağlam stratejiler sunmaktadır. Gizlilik teknolojisi literatürü, kullanıcı merkezli gizlilik politikaları ve gizlilik korumasına yönelik politika tabanlı yaklaşımlar da dahil olmak üzere çok çeşitli konuları kapsamaktadır. Gizlilik yöntemleri ve literatüre katkılar bu bölümde incelenmektedir.

Gürses ve ark. (2011), gizlilik teknolojisi tekniklerini çevrimiçi cihazlara uygulayarak gizlilik politikası kavramlarının gerçek dünyadaki uygulamalarını incelemiştir. Çalışmada, erken planlamanın gizlilik hususlarını nasıl etkileyebileceği tartışılmıştır. IoT cihazlarının sınırlı işlem yetenekleri için yeterli gizlilik koruması oluşturmaya odaklanılmıştır. Özellikle gizlilikle ilgili tasarım süreçleri aracılığıyla sistem güvenliğinin geliştirilebileceği vurgulanmıştır.

Velioğlu (2023), gizlilik artırıcı teknolojiler ve bunların kullanım örneklerini ele almıştır. Çalışmada, IoT cihazlarının gizlilik gereksinimlerini karşılamak için geliştirilen teknolojiler incelenmiş ve bu teknolojilerin kullanıcı merkezli bir yaklaşımla nasıl optimize edilebileceği tartışılmıştır. Özellikle, diferansiyel gizlilik ve homomorfik şifreleme gibi yöntemlerin pratik uygulamaları analiz edilmiştir. Bu çalışma ile gizlilik artırıcı teknolojilerin IoT ve büyük veri ortamlarındaki etkisini değerlendiren bir çerçeve sunulmuştur.

Cranor ve Garfinkel (2004), kullanılabilirlik ile güvenlik arasındaki boşluğu dolduran gizlilik teknolojisi stratejilerini tartışmaktadır. Çalışmada, güvenlik sisteminin kullanım kolaylığının gizlilik koruma stratejilerini nasıl etkilediği ve gizlilik teknolojisi önlemlerinin kullanılabilirliğe nasıl dahil edilebileceği incelenmiştir. Çalışma, ilgili alanda gelecekteki araştırmalar için teorik bir temel sağlamakta ve temel kullanıcı deneyimlerine öncelik veren gizlilik koruma stratejilerinin benimsenmesinin fizibilitesini ortaya koymaktadır.

IoT uygulamalarında gizlilik farkındalığını artırmaya yönelik bir çerçeve Perera ve ark. (2015) tarafından sağlanmaktadır. Çalışmada internetteki gizlilik teknolojisi stratejileri hakkında bilgiler verilmiş ve bu stratejilerin kullanıcı gizliliğini nasıl geliştirebileceği tartışılmıştır. Gizliliğe öncelik veren IoT cihazlarını destekleyen öneriler sunulmuştur (Perera ve ark., 2020).

Alhirabi ve ark. (2022), IoT uygulamalarında gizlilik koruma stratejilerini geliştirmek için kullanılan gizlilik desenlerini incelemiştir. Çalışmada, mahremiyet mühendisliği yaklaşımları için pratik bir rehber sunulmuş ve bu yaklaşımların geliştirici perspektifinden nasıl uygulanabileceği tartışılmıştır. Çalışmada, IoT bağlamında gizlilik tasarım desenlerinin etkinliğini artırmaya yönelik öneriler sunulmuştur.

Bu bölümde, mahremiyet mühendisliği yöntemlerinin IoT ve büyük veri bağlamındaki uygulamaları ele alınmıştır. Çalışmalar, gizlilik gereksinimlerini sistem tasarımına entegre etmenin, hem bireysel mahremiyeti hem de veri güvenliğini artırmak için güçlü bir araç olduğunu ortaya koymaktadır.

3. LİTERATÜRDEKİ ÇALIŞMALARIN KARŞILAŞTIRMASI

Bu bölümde Tablo 1'de gösterildiği gibi literatürdeki büyük veri ve IoT ortamlarındaki gizliliği koruma stratejilerine odaklanan önemli çalışmaların karşılaştırması yapılmıştır. İncelenen çalışmaların yayımlanma yılları, yöntemleri ve sonuçları tabloda özetlenmiştir. Bu karşılaştırmanın amacı farklı yaklaşımlarda kullanılan yöntemleri ve sonuçlarını incelemek ve daha sonraki araştırmalar için bir yol haritası çizmektedir.

Tablo 1. Literatürdeki çalışmaların karşılaştırılması.

Çalışma	Yıl	Kullanılan Yöntemler	Sonuçlar
Cranor ve Garfinkel	2004	Güvenlik ve kullanılabilirlik	Kullanıcı dostu güvenlik uygulamaları
Yee	2004	Güvenlik ve kullanılabilirliği sıraya koyma	Kullanıcıların beklentilerini ele alan ve atama eylemlerine dayalı yetkilendirme
Gürses ve ark.	2011	Gizlilik mühendisliği yöntemleri	Etkin gizlilik tasarımı ve uygulama
Xu ve ark.	2014	Büyük veride bilgi güvenliği	Gizlilik ve veri madenciliğinde başarı
Perera ve ark.	2015	IoT'de büyük veri gizliliği	IoT cihazlarında veri anonimleştirme
Yang ve ark.	2016	Çoklu bulut tabanlı gizlilik koruma	Yüksek gizlilik, düşük veri kaybı oranı
Polat ve ark.	2017	Veri tabanı anonimleştirme	Verilerin anonimlik düzeyini artırma
Wang ve ark.	2018	IoT'de güvenlik ve gizlilik özel sayısı	IoT güvenlik sorunlarının kapsamlı analizi
Du ve ark.	2018	MEC ile anonimleştirme	IoT verilerinde güvenlik artırımı, veri kaybında azalma
Seliem ve ark.	2018	IoT için anonimleştirme ve güvenlik yöntemleri	Yüksek gizlilik ve saldırı önleme
Ali ve ark.	2018	Sensör düğümlerinde veri toplama ve anonimleştirme	Kaynak sınırlamalarına rağmen yüksek gizlilik
Eyupoglu ve ark.	2018	Kaos ve pertürbasyon tekniklerine dayalı büyük veri anonimleştirme	Etkin gizlilik korumalı veri yayınlama
Binjubeir ve ark.	2019	Büyük veri gizlilik koruma araçları	Gelişmiş güvenlik ve kullanıcı mahremiyeti
Perera ve ark.	2020	IoT uygulamaları için gizlilik farkındalığı	IoT kullanıcıları için farkındalık çözümleri
Al-Slais	2020	Gizlilik mühendisliği yöntemleri	Etkin gizlilik tasarımı ve saldırı önleme
Kara ve Eyüpoğlu	2020	Sağlık 4.0 için gizlilik artırıcı teknolojiler	Sağlık verilerinde mahremiyetin korunması
Kiani ve Taş	2021	IoT ve kablosuz ağlarda saldırı tespiti	Güvenlik açıklarını belirlemede yüksek başarı oranı
Alhirabi ve ark.	2022	IoT geliştiricileri için gizlilik desenleri	Gizlilik odaklı yazılım geliştirme
Gümüş ve Eyüpoğlu	2022	Anonimleştirme teknikleri ve saldırı türleri	Büyük veri ortamlarında etkili saldırı tespiti
Ahmetoglu ve Das	2022	Büyük veride anonimleştirme ve saldırı teknikleri	Büyük veri ortamında saldırı önleme
Torre ve ark.	2023	IoT cihazlarında gizlilik koruma teknikleri	Gizlilik artırımı, IoT cihazlarında veri güvenliği
Sen ve Dasgupta	2023	Veri akışında güvenlik ve gizlilik yöntemleri	Güvenli veri akışı, veri gizliliği sağlama
Velioğlu	2023	Gizlilik artırıcı teknolojiler	Verilerin anonimliğini artırma, saldırı riskini azaltma
Dhinakaran ve ark.	2024	Yapay zeka entegrasyonu ile veri koruma	Yapay zeka ile geliştirilmiş güvenlik ve gizlilik
Uluç ve Eyüpoğlu	2024	Akıllı saatlerin siber güvenlik ve mahremiyet açısından incelenmesi	Güvenlik ve mahremiyet riskleri

4. SONUÇLAR

Bu çalışmada, IoT ve büyük veri konularındaki mevcut gizlilik koruma stratejileri incelenmiştir. Literatür taraması, diferansiyel gizlilik ve homomorfik şifreleme gibi karmaşık tekniklerin veri gizliliğini önemli ölçüde iyileştirdiğini göstermektedir. Özellikle sağlık ve endüstriyel IoT gibi alanlarda gizliliğin korunması için *k*-anonimlik, *l*-çeşitlilik ve *t*-yakınlık gibi anonimleştirme tekniklerine ihtiyaç duyulduğu görülmektedir. Ayrıca IoT teknolojilerinin güvenliğini artırmanın etkili bir yolu, cihazların sınırlı kullanım durumları için tasarlanmış gizlilik teknolojisi tekniklerini kullanmaktır. Yapay zeka entegrasyonu, veri analizi doğruluğunu korurken gizliliği artırabilen bir alternatif örneğidir. Sonuç olarak, büyük veri ve IoT ekosistemlerinde mahremiyetin sağlanması, sürekli gelişen bir alan olarak dikkat çekmektedir. Bu çalışma, gelecekteki araştırmalar için teorik bir temel oluşturmakta ve pratik uygulamalara yönelik öneriler sunmaktadır. Daha etkili ve ölçeklenebilir gizlilik koruma çözümleri geliştirmenin, bu teknolojilerin güvenli ve etik bir şekilde kullanılmasını destekleyeceği düşünülmektedir.

KAYNAKLAR

Ahmetoglu, H., & Das, R. (2022). A comprehensive review on detection of cyber-attacks: data sets, methods, challenges, and future research directions. *Internet of Things*, *20,* 100615.

Al-Slais, Y. (2020, December). Privacy engineering methodologies: A survey. In *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)* (pp. 1-6). IEEE.

Alhirabi, N., Beaumont, S., Rana, O., & Perera, C. (2022, September). Privacy-patterns for IoT application developers. In *Adjunct Proceedings of the 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing and the 2022 ACM International Symposium on Wearable Computers* (pp. 7-9).

Ali, I., Khan, E., & Sabir, S. (2018). Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things: A review. *Future Computing and Informatics Journal*, *3*(1), 41-50.

Binjubeir, M., Ahmed, A. A., Ismail, M. A. B., Sadiq, A. S., & Khan, M. K. (2019). Comprehensive survey on big data privacy protection. *IEEE Access*, *8*, 20067-20079.

Dhinakaran, D., Sankar, S. M., Selvaraj, D., & Raja, S. E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. arXiv preprint arXiv:2401.00794.

Du, M., Wang, K., Chen, Y., Wang, X., & Sun, Y. (2018). Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things. *IEEE Communications Magazine*, *56*(8), 62-67.

Eyüpoğlu, C. (2018). *Büyük veride etkin gizlilik koruması için yazılım tasarımı* (Doctoral dissertation, Doktora tezi) (İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul).

Eyüpoğlu, C., Aydın, M. A., Sertbaş, A., Zaim, A. H., & Öneş, O. (2017). Büyük veride kişi mahremiyetinin korunması. *Bilişim Teknolojileri Dergisi*, *10*(2), 177-184.

Eyupoglu, C., Aydin, M. A., Zaim, A. H., & Sertbas, A. (2018). An efficient big data anonymization algorithm based on chaos and perturbation techniques. *Entropy*, *20*(5), 373.

Gümüş, H. T., & Eyüpoğlu, C. (2022). Büyük Veride Anonimleştirme Teknikleri ve Saldırı Türleri: Uygulama Örnekleri. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, *21*(42), 422-441.

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. *Computers, Privacy & Data Protection*, *14*(3), 25.

Jiang, B., Li, J., Yue, G., & Song, H. (2021). Differential privacy for industrial internet of things: Opportunities, applications, and challenges. *IEEE Internet of Things Journal*, *8*(13), 10430-10451.

Kara, B. C., & Eyupoglu, C. (2021, October). Anonymization methods for privacy-preserving data publishing. In *The International Conference on Artificial Intelligence and Applied Mathematics in Engineering* (pp. 145-159). Cham: Springer International Publishing.

Kara, B. C., & Eyüpoğlu, C. (2020, October). Sağlık 4.0'da Mahremiyet ve Güvenlik Sorunları/Privacy and Security Problems in Healthcare 4.0. In *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 1-12). IEEE.

Kara, B. C., & Eyüpoğlu, C. (2023). A New Privacy-Preserving Data Publishing Algorithm Utilizing Connectivity-Based Outlier Factor and Mondrian Techniques. *Computers, Materials & Continua*, *76*(2), 1515-1535.

Kara, B. C., Eyüpoğlu, C., Uysal, S., & Bayraklı, S. (2023). Collection of an e-Health Dataset and Anonymization with Privacy-Preserving Data Publishing Algorithms. *Electrica*, *23*(3), 658-665.

Kiani, F., & Taş, O. (2021). Nesnelerin İnterneti (IoT) ve Kablosuz Algılayıcı Ağların Güvenliğine Yapılan Saldırıların Tespit Edilmesi ve Önlenmesi: Detection and Prevention of Attacks on the Internet of Things (IoT) and Wireless Sensor Networks. *Politeknik Dergisi*, *24*(1), 219-235.

Perera, C., Barhamgi, M., Bandara, A. K., Ajmal, M., Price, B., & Nuseibeh, B. (2020). Designing privacy-aware internet of things applications. *Information Sciences*, *512*, 238-257.

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the internet of things era. *IT professional*, *17*(3), 32-39.

Polat, H., Okkalıoğlu, B. D., & Koç, M. (2017). Bölünmüş Veri-Tabanlı Gizliliği Koruyan Ortak Filtreleme Sistemlerinde Gizli Verinin Elde Edilmesi. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *32*(1), 53-64.

Seliem, M., Elgazzar, K., & Khalil, K. (2018). Towards Privacy Preserving IoT Environments: A Survey. *Wireless Communications and Mobile Computing*, *2018*(1), 1032761.

Sen, J., & Dasgupta, S. (2023). Data Privacy Preservation on the Internet of Things. arXiv preprint arXiv:2304.00258.

Torre, D., Chennamaneni, A., & Rodriguez, A. (2023). Privacy-preservation techniques for IoT devices: a systematic mapping study. *IEEE Access*, *11*, 16323-16345.

Uluç, C., & Eyüpoğlu, C. (2024). Çocuklara Yönelik Akıllı Saatlerin Siber Güvenlik ve Mahremiyet Açısından İncelenmesi. *İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi*, *7*(1), 77-87.

Velioğlu, İ. (2023). *Gizlilik artırıcı teknolojiler ve kullanım örnekleri* (Master's thesis, Lisansüstü Programlar Enstitüsü).

Wang, H., Zhang, Z., & Taleb, T. (2018). Special issue on security and privacy of IoT. *World Wide Web*, *21*, 1-6.

Cranor, L. F., & Garfinkel, S. (2004). Guest Editors' Introduction: secure or usable?. *IEEE Security & Privacy*, *2*(5), 16-18.

Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2014). Information security in big data: privacy and data mining. *IEEE Access*, *2*, 1149-1176.

Yang, L., Humayed, A., & Li, F. (2016, December). A multi-cloud based privacy-preserving data publishing scheme for the internet of things. In *Proceedings of the 32nd annual conference on computer security applications* (pp. 30-39).

Yee, K. P. (2004). Aligning security and usability.*IEEE Security & Privacy*, *2*(5), 48-55.

TEŞEKKÜR ve BEYANLAR

Yazarlar çalışmaya eşit oranda katkı sağlamıştır. Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır. Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.