Journal of the Faculty of Engineering and Architecture of Gazi University 35:1 (2020) 355-368

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

OAN: outlier record-oriented utility-based privacy preserving model

Yavuz Canbay[1*], Yılmaz Vural[2], Şeref Sağıroğlu[1]

[1]Department of Computer Engineering, Gazi University, Ankara, 06570, Turkey
[2]Turkish Data Protection Authority, Ankara, 06520, Turkey

Highlights:

- Developing a new privacy preserving model
- Utility-based model
- Outlier record-oriented model

Keywords:

- Data utility
- Outlier record management
- Privacy preserving

Article Info:

Research Article
Received: 04.10.2018
Accepted: 06.03.2019

DOI:

10.17341/gazimmfd.467390

Correspondence:

Author: Yavuz Canbay
e-mail: yavuzcanbay@gazi.edu.tr
phone: +90 312 582 3130

Graphical/Tabular Abstract

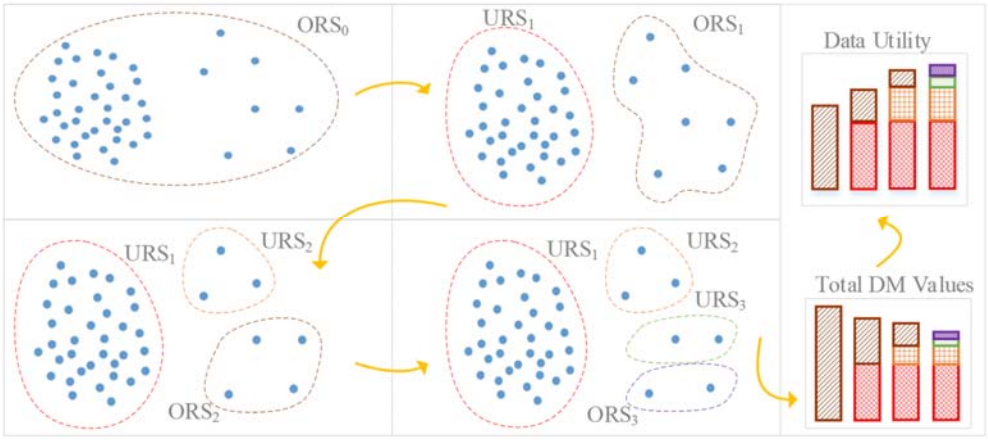


Figure A. General representation of the proposed model

Purpose: In this paper, a new outlier record-oriented utility-based privacy preserving model was proposed. The existence of outliers in data set decreases data utility in anonymization. Hence, outliers should be managed in the anonymization process. In traditional management approaches, outliers are detected after anonymization and they are partially or completely removed from the published data set. However, detection of outliers after anonymization increases computational cost and the removal of the outliers from the data set reduces total data utility. In this study, a new outlier-oriented utility-based privacy preserving model named as OAN, which reduces the computational cost by detecting outliers before anonymization and increases data utility by using all data, was proposed.

Theory and Methods:
In the proposed model, data is divided into two subsets which are named as utility record set (URS) and outlier record set (ORS). URS includes normal data that presents high data utility. ORS is the set of outlier records that decreases total data utility. In order to increase total data utility, ORS is divided into two new subsets such as URS and ORS sets recursively. If a stopping criteria is met, this recursion stops and finally anonymized data is released. Local Outlier Factor was employed for outlier detection and anonymization was performed by using Mondrian algorithm. DM and AECS metrics were used to evaluate the information loss of the proposed model.

Results:
In the experiments, Adult data set was used to test the proposed model. DM and AECS metrics were employed to measure data utility. It was observed that the results of the proposed model presented better results than classical Mondrian. The results showed that OAN increases total data utility while preserving data privacy. In addition, it was showed that the proposed model is computational cost-effective compared to another utility based anonymization model.

Conclusion:
In this paper, a new outlier record-oriented utility-based privacy preserving model was proposed, tested and verified. Two information metrics and Adult data set were employed in the experiments and the results showed that the proposed model is an effective solution in terms of computational cost and data utility.

Journal of the Faculty of Engineering and Architecture of Gazi University 35:1 (2020) 355-368

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

OAN: aykırı kayıt yönelimli fayda temelli mahremiyet koruma modeli

Yavuz Canbay[1]*, Yılmaz Vural[2], Şeref Sağıroğlu[1]

[1]Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570, Ankara, Türkiye
[2]Kişisel Verileri Koruma Kurumu, Nasuh Akar Mahallesi Ziyabey Cad. 1407. Sok. No:4, 06520, Ankara, Türkiye

Ö N E Ç I K A N L A R

- Yeni bir mahremiyet koruma modeli geliştirme
- Fayda temelli model
- Aykırı kayıt yönelimli model

Makale Bilgileri

Araştırma Makalesi
Geliş: 04.10.2018
Kabul: 06.03.2019

DOI:
10.17341/gazimmfd.467390

Anahtar Kelimeler:
Veri faydası,
aykırı kayıt yönetimi,
mahremiyet koruma

ÖZET

Veri mahremiyeti, mahremiyet seviyesi ile veri faydası arasındaki en iyi dengeyi bulmaya çalışan zor bir problemdir. Anonimleştirme, veri mahremiyetini korumada yaygın olarak kullanılan fayda temelli çözümlerin başında gelir. Veri kümesi içerisinde bulunabilecek aykırı veriler, anonimleştirme işleminde toplam veri faydasını düşürür. Bundan dolayı aykırı verilerin anonimleştirme sürecinde yönetilmesi gerekir. Geleneksel yaklaşımlarda aykırı veriler, anonimleştirme sonrası tespit edilerek yayınlanacak veri kümesinden kısmen veya tamamen çıkarılır. Ancak, aykırı verilerin anonimleştirme sonrası tespit edilmesi hesaplama maliyetini arttırırken, bu verilerin yayınlanacak veri kümesinden çıkarılması ise toplam veri faydasını düşürür. Bu çalışmada, aykırı verileri anonimleştirme öncesi tespit ederek hesaplama maliyetini düşüren ve tüm verileri kullanarak toplam veri faydasını arttıran aykırı veri yönelimli fayda temelli yeni bir mahremiyet koruma modeli (OAN) önerilmiştir. OAN modelinin hesaplama maliyeti açısından etkin bir çözüm olduğu, fayda temelli başka bir modelle kıyaslanarak gösterilmiştir. Ayrıca yapılan deneyler sonucunda, önerilen modelin veri mahremiyetini koruyarak toplam veri faydasını arttırdığı gözlemlenmiştir.

OAN: outlier record-oriented utility-based privacy preserving model

H I G H L I G H T S

- Developing a new privacy preserving model
- Utility-based model
- Outlier record-oriented model

Article Info

Research Article
Received: 04.10.2018
Accepted: 06.03.2019

DOI:
10.17341/gazimmfd.467390

Keywords:
Data utility,
Outlier record management,
Privacy preserving

ABSTRACT

Data privacy is a hard trade-off problem between privacy level and data utility. Anonymization is one of the most commonly used utility-based solutions for preserving data privacy. The existence of outliers in data set decreases data utility in anonymization. Hence, outliers should be managed in the anonymization process. In traditional approaches, outliers are detected after anonymization and they are partially or completely removed from the published data set. However, detection of outliers after anonymization increases computational cost and the removal of the outliers from the data set reduces total utility. In this study, a new outlier record-oriented utility-based privacy-preserving model named as OAN, which reduces the computational cost by detecting outliers before anonymization and increases data utility by using all data, was proposed. It was shown that OAN is an effective solution in terms of computational cost compared to another utility-based model. According to the experimental results, it was observed that the proposed model increased total data utility while preserving the privacy of data.

*Sorumlu Yazar/Corresponding Author: yavuzcanbay@gazi.edu.tr, yilmazvural@gmail.com, ss@gazi.edu.tr / Tel: +90 312 582 3130

1. GİRİŞ (INTRODUCTION)

Günümüzde pek çok kurum (veri sorumlusu) hizmet verdiği muhataplarına (müşteri, hasta, kullanıcı, firma vb.) ait çeşitli verileri toplamakta ve bunları depolamaktadır. Bu veriler içerisinde bireyi doğrudan veya dolaylı olarak tanımlayabilecek kişisel veriler de yer alabilmektedir. Veri sorumluları, görevlerini yerine getirmek ve muhataplarına daha iyi hizmet sunmak (model ve örüntü çıkarmak, planlamalar yapmak, politikalar oluşturmak, karar verme mekanizmalarını geliştirmek vb.) amacıyla verileri işlemektedir. İşlenen bu verilerden yüksek seviyede değer üretilmesi için verinin kişi, kurum ve kuruluşlarla paylaşılması gerekir. Ancak mahremiyet ihlali kaygı ve endişesi, veri sorumlularının işlediği verilerini paylaşmasını olumsuz yönde etkiler.

Veri paylaşımındaki en yaygın yöntemlerin başında veri yayınlama gelmektedir. Veri sorumlularının yayınladığı veriler içerisinde yer alan hassas bilgiler, bu verilerin yeterli düzeyde korunmasını gerektirir. Yayınlanacak veri kümesi herhangi bir mahremiyet koruyucu önlem alınmadan paylaşılırsa, farklı saldırı yöntemleri kullanılarak bu veri kümelerinde yer alan kişilerin kimlikleri ifşa edilebilir. Tekil-tanımlayıcı olarak nitelendirilen ve bireyi doğrudan tanımlayan alanların (kimlik numarası, adı soyadı vb.) yayınlanan verilerden çıkarılması kimliksizleştirme olarak adlandırılır. Kimliksizleştirme yaklaşımının veri sahiplerinin mahremiyetini tam olarak koruyamadığı Sweeney tarafından yapılan çalışmada gösterilmiştir [1]. Sweeney, kimliksiz olarak yayınlanan sağlık verilerini oy verileri ile cinsiyet-posta kodu-doğum tarihi alanları üzerinden eşleştirerek Amerika nüfusunun %87'sinin kimlik bilgilerini ifşa edilebileceği göstermiştir. 2006 yılında ise AOL firması, 650 bin kullanıcıya ait 20 milyon arama sorgusu verisini kullanıcı kimliği ve IP numarası bilgilerini silerek kimliksiz olarak yayınlanmış ancak birkaç gün içerisinde bu sorguların kimlere ait olduğu araştırmacılar tarafından tespit edilmiştir [2, 3].

Kimliksizleştirme yöntemiyle alınan mahremiyet koruma önlemine rağmen ihlallerin yaşanması, bu yöntemin yeterli olmadığını ve daha gelişmiş önlemlere ihtiyaç duyulduğunu ortaya koymuştur. Bu ihtiyacı gidermek adına anonimleştirme kavramı ortaya çıkmıştır. Anonimleştirme, eşleştirme sonucu meydana gelen ifşa saldırılarına karşı koruma sağlayan fayda temelli bir yöntemdir. Literatürde, anonimleştirme gereksinimlerinin karşılanmasında bazı temel mahremiyet modellerinin (k-Anonimlik, l-Çeşitlilik, t-Yakınlık ve δ-Mevcudiyet) olduğu ve özellikle kimlik, öznitelik ve üyelik ifşalarına karşı koruma sağlamak amacıyla bu modellerin çoğunlukla birlikte kullanıldıkları görülmüştür [4].

Anonimleştirmede, toplam veri faydasını olumsuz etkileyen aykırı verilerin anonimleşme sürecinde yönetilmesi gerekir. Aykırı verilerin yönetilmesi amacıyla literatürde kullanılan mevcut yaklaşımlar aşağıda listelenmiştir;

1. aykırı verilerin anonimleştirme öncesi tespit edilerek tamamının yayınlanacak veri kümesinden çıkarılması [5],
2. aykırı verilerin anonimleştirme sonrası tespit edilerek global aykırı verilerin yayınlanacak veri kümesinden çıkarılması ve yerel aykırı verilerin en yakın aykırı olmayan gruplara eklenmesi [6-8],
3. aykırı verilerin anonimleştirme sonrası tespit edilerek fayda elde edilebileceklerin yeniden değerlendirilmesi ve arta kalan aykırı verilerin yayınlanacak veri kümesinden çıkarılması [9-11].

Yukarıda belirtilen 1 ve 2 numaralı yaklaşımlarda sadece veri mahremiyetinin korunması, 3 numaralı yaklaşımda ise veri mahremiyetinin korunarak aynı zamanda veri faydasının arttırılması amaçlanmıştır.

Literatürde, aykırı verilerin normal verilerden ayırt edilebilmesi amacıyla uzaklık tabanlı [6-8] ve taksonomi ağacı tabanlı [9-12] yaklaşımlar kullanılmıştır. Aykırı verileri uzaklık tabanlı tespit eden yaklaşımlarda, öznitelik uzayında temsil edilen veriler üzerinde bir uzaklık fonksiyonu kullanılarak aykırı veriler belirlenir. Ancak bu yaklaşım yerel aykırı verilerin belirlenmesinde yetersiz kaldığı için muhtemel veri faydasının da düşmesine neden olur. Taksonomi ağacı tabanlı aykırı veri tespit yaklaşımlarında ise taksonomi ağacının kullanıcı tanımlı olması aykırı verilerin belirlenmesini olumsuz olarak etkiler.

Bu çalışmada yukarıda belirtilen problemleri çözmek için, aykırı verileri yoğunluk tabanlı bir yaklaşımla ve anonimleştirme öncesi ayırt edebilen ve tüm aykırı verileri kullanan fayda temelli yeni bir anonimleştirme modeli önerilmiştir. Bir verinin yoğunluğunun yüksek olması, yakın komşuluğunda çok sayıda birbirine oldukça benzer verilerin olduğunu gösterir. Yoğunluk olarak birbirine yakın yarı-tanımlayıcı değerlerine sahip veriler kullanılarak eşlenik sınıflar oluşturulabilir. Önerilen modelde aykırı veri tespitinde yoğunluk tabanlı bir yaklaşımın kullanılmasının uygun olacağı değerlendirildiğinden Yerel Aykırılık Faktörü (Local Outlier Factor-LOF) [13] algoritmasından faydalanılmıştır. LOF algoritması, veri dağılımından bağımsız olarak aykırı verileri tespit etmesi, veri dağılımı hakkında herhangi bir ön kabul yapmaması, parametre karmaşıklığının az olması ve yerel bir model olmasından dolayı bu çalışmada tercih edilmiştir.

Önerilen model ile aykırı veri yönetimi yapılarak veri faydası arttırılmış ve hesaplama maliyeti düşürülmüştür. Önerilen OAN modelinin hesaplama maliyeti açısından daha etkin bir çözüm olduğu aykırı verileri dikkate alan ve güncel bir model olan ρ-Gain [11] ile kıyaslanarak gösterilmiştir. Ayrıca, OAN modelinin doğruluğunu test etmek amacıyla bir deney düzeneği oluşturulmuş ve bu düzenekte iki farklı bilgi metriğine göre sonuçlar elde edilmiştir. Makalenin ikinci bölümünde çalışmanın daha iyi anlaşılabilmesi amacıyla temel kavramlar verilmiş, üçüncü bölümünde mahremiyeti hedef alan tehditler ve mahremiyet koruma

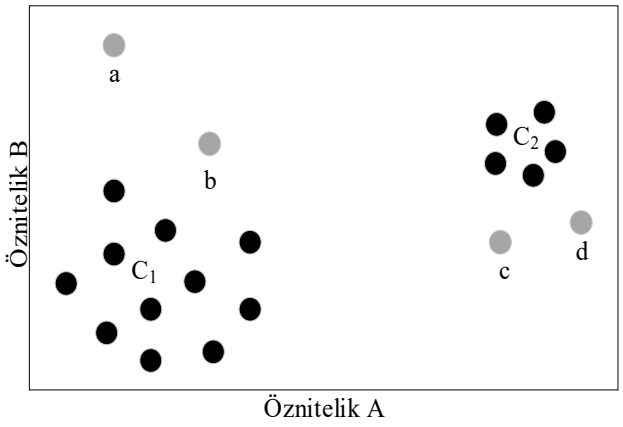
yaklaşımları açıklanmıştır. Dördüncü bölümde, önemli anonimleştirme algoritmaları ve sıklıkla kullanılan bilgi metrikleri özetlenmiştir. Önerilen model beşinci bölümde tanıtılmış, modelin etkinliğini göstermek üzere yapılan deneysel çalışmalara ise altıncı bölümde yer verilmiştir. Çalışmanın son bölümünde ise sonuçlar tartışılmıştır.

2. TEMEL KAVRAMLAR (BASIC DEFINITIONS)

Bu çalışma kapsamında ele alınan aykırı veri, normal veri, veri faydası ve fayda metriği kavramları aşağıda açıklanmıştır.

Aykırı veri: V veri kümesi, $v \in V$, $t > 0$ bir eşik değeri ve $LOF()$ bir yoğunluk fonksiyonu olmak üzere; eğer $LOF(v) \geq t$ ise v_A aykırı veridir.

Öznitelik uzay düzleminde temsil edilen herhangi bir verinin yoğunluğunun komşularının yoğunluğundan daha düşük olması ilgili veriyi aykırı veri olarak etiketlendirir. Aykırı verilerin anonimleştirme kapsamında toplam veri faydasını olumsuz etkilediği çeşitli çalışmalarda rapor edilmiştir. Bu çalışmada, yoğunluk tabanlı aykırı veriler dikkate alınmıştır. Şekil 1'de iki boyutlu öznitelik uzayında a, b, c ve d noktaları dört farklı aykırı veri olarak temsil edilmiştir. a ve b verileri kendilerine en yakın küme olan C_1 kümesindeki verilerden, c ve d verileri ise kendilerine en yakında olan C_2 kümesindeki verilerden yoğunluk olarak daha az olduğu için aykırı veri olarak kabul edilir.



Şekil 1. Yoğunluk tabanlı aykırı ve normal veri örneği
(An example for density based outlier and normal data)

Normal veri: V_A anonim veri kümesi, $v_A \in V_A$ ve $t > 0$ bir eşik değeri olmak üzere; eğer v_A aykırı veri değil ise v_A normal veridir. Öznitelik uzay düzleminde temsil edilen herhangi bir verinin yoğunluğu bir t eşik değerinden daha düşük ise ilgili veri normal veri olarak etiketlendirilir. Şekil 1'de C_1 ve C_2 kümesinde yer alan veriler normal veri olarak kabul edilmektedir. Anonimleştirme çalışmalarında normal veri, veri faydası sunan veri kümesi olarak kabul edilir.

Veri faydası: V orijinal veri kümesi, V_A anonim veri kümesi, $Yakınlık()$ bir bilgi kaybı ölçüm fonksiyonu ve $u \geq 0$ olmak üzere; $u = Yakınlık(V, V_A)$ için, u veri faydasıdır.

Literatürde bulunan genel bilgi metrikleri $Yakınlık()$ fonksiyonunda kullanılabilir. Mondrian algoritması DM ve AECS metriklerini desteklediği için bu çalışmada $Yakınlık()$ fonksiyonu için bu iki metrik kullanılmıştır. DM ve AECS metrik değerleri veri faydası ile ters orantılıdır. Yani bu metriklerin değeri artarken veri faydası azalır, bu metriklerin değeri azalırken de veri faydası artar. V orijinal veri kümesi, U orijinal veri kümesinin DM değeri, U' aykırı veri yönetimi sonrası elde edilen DM değeri, N_i mevcut iterasyondaki normal veri kümesi, O_n son iterasyondaki aykırı veri kümesi, n aykırı verilerin parçalanma sayısı ve $V = N \cup O$ olmak üzere aykırı veri yönetimi ile veri faydasının arasındaki ilişkiyi DM metriği cinsinden gösteren bir B karar kuralı aşağıda oluşturulmuştur.

Başlangıç durumu: $U = DM(V)$
Aykırı veri yönetimi sonrası: $U' = \sum_{i=0}^{n} DM(N_i) + DM(O_n)$

$$B = \begin{cases} 1, eğer\ U' < U \\ 0, diğer\ durumda \end{cases}$$

B karar kuralına dayanarak, kuralın çıktısı eğer 1 ise veri faydasının arttığı, 0 ise veri faydasının aynı kaldığı veya azaldığı görülür.

Fayda metriği: anonimleştirilen verinin faydasını ölçmede kullanılan ölçektir. Aykırı verilerin normal verilerden ayrı olarak ele alınması eşlenik sınıf büyüklüğünü ve bu sınıflardaki ortalama eleman sayılarını doğrudan etkileyeceği için, doğru metriklerin kullanımı önemlidir.

Yukarıda verilen tanımlar dikkate alınarak bu çalışmada, tüm veri kümesi aykırı ve normal olmak üzere yinelemeli olarak iki alt kümeye parçalanmakta, her bir kümenin veri faydası bir fayda metriği kullanılarak ölçülmektedir.

3. VERİ MAHREMİYETİNİ HEDEF ALAN TEHDİTLER VE KORUMA YAKLAŞIMLARI (THREATS ON DATA PRIVACY AND PRIVACY PRESERVING APPROACHES)

Veri mahremiyeti ihlalleri, bireyleri doğrudan hedef alarak mağduriyet ve ayrımcılık yaşanmasına yol açtığı için saldırganların ilgisini sıklıkla çekmektedir. Saldırgan, sahip olduğu arka plan bilgisini yayınlanan veri kümeleri ile belirli öznitelikler üzerinde birleştirerek kurbanın kimlik ve hassas bilgilerini ifşa edebilir. Böylesi ihlallerin yaşanmaması, saldırılara karşı yeterli önlemlerin alınması ve farkındalığın arttırılması amacıyla veri mahremiyetini hedef alan tehditler, mahremiyet koruyucu yaklaşımlar ve bu yaklaşımların uygulanmasını sağlayan modellerin bilinmesi gerekir.

3.1 Veri Mahremiyetini Hedef Alan Tehditler (Threats on Data Privacy)

Arka plan bilgileri ile veri bağlama yöntemleri, veri mahremiyetine yönelik tehditlerin başında gelir [14]. Kurban hakkında bir ön bilgi sunan arka plan bilgilerini yayınlanan diğer veri kümeleri ile bağlayan saldırgan, veri eşleştirmesi yaparak veri sahiplerini ifşa edebilir. Bu eşleştirmeler genel olarak kayıt, hassas öznitelik veya tablo düzeyindedir [15, 16]. Arka plan bilgileri ve veri bağlama yöntemleri aşağıda kısaca açıklanmaktadır.

Arka plan bilgileri: çeşitli kurum ve kuruluşlar tarafından yayınlanan verilerden, sosyal ağlardan, çeşitli çevrim içi sitelerden, gerçek dünyadaki sosyal ilişkilerden ve diğer yollardan elde edilebilen bilgilerdir. Saldırgan, kurban hakkında önceden bilgi sahibi olmak için bu bilgileri kullanır. Yayınlanan veri kümelerinin sahiplerini çeşitli yöntemler kullanarak ifşa etmek için bu ön bilgilerden yararlanılır [17].

Veri bağlama: yayınlanan bir veya daha fazla veri kümesinin kayıt, hassas öznitelik veya tablo bazında eşleştirilmesiyle gerçekleştirilir. Bu tehdit sonucu oluşabilecek ihlallerden bazıları aşağıda listelenmiştir;

- Kimlik ifşası: arka plan bilgisine sahip bir saldırganın, kamuya açık kimlik bilgileri içeren veri kümelerini yayınlanmış kimliksiz veri kümeleri ile yarı-tanımlayıcılar üzerinden kayıt düzeyinde eşleştirmesi sonucu meydana gelir. Saldırgan, yayınlanan kimliksiz veri içerisindeki kurbana ait hassas bilgileri öğrenerek kurbanın hassas bilgilerini kimliği ile beraber ifşa eder [18].
- Hassas öznitelik ifşası: arka plan bilgisine sahip saldırgan, yayınlanan veri kümesindeki hassas öznitelik değerlerinin homojen dağılımına bakarak kurbanın hassas bilgilerini öğrenebilir. Örneğin, yayınlanan veri kümesinde kurbanın da yer aldığını bilen bir saldırgan, bu veri kümesinden hangi kaydın kurbana ait olduğunu öğrenemez ancak hassas öznitelik değerinin aynı olmasından dolayı kimliğini tanımlayamadığı kurbanının hassas bilgisini ifşa edebilir [2].
- Üyelik ifşası: yayınlanan veri kümesi içerisinde kurbanın da yer aldığını bilen bir saldırgan, kurban ile yayınlanan bu veri kümesi arasında bir ilişki ortaya çıkararak üyelik ifşası gerçekleştirebilir. Herhangi bir bilgiyi ifşa edemeyen saldırgan, yayınlanan veriye göre üst seviye çıkarımlar yapabilir [19]. Sonraki süreçte saldırgan, üyelik ifşası sonucu elde ettiği bilgiyi geliştirerek arka plan bilgisini arttırmayı, bu bilgileri kullanacağı yayınlanan diğer veri kümelerini bularak kurbanın kimlik ve hassas öznitelik bilgisini ifşa etmeyi amaçlar.

3.2. Veri Mahremiyeti Koruma Yaklaşımları
(Privacy Preserving Approaches)

Veri mahremiyetini hedef alan tehditleri bertaraf etmek için literatürde çeşitli mahremiyet koruma yaklaşımları geliştirilmiştir. Şifreleme ve anonimleştirme, veri mahremiyetini korumada kullanılan temel yaklaşımlardır [20]. Şifreleme; hassas veriye yetkisiz kişilerin erişimini engellemek için kullanılan, verinin gizlilik ve bütünlük ilkelerini koruyan ve en yüksek seviyede veri mahremiyeti sunan bir yaklaşımdır. Herhangi bir veri faydası sunmamasından dolayı mahremiyet korumalı veri yayınlama kapsamında kullanılmamaktadır [20]. Anonimleştirme ise; mahremiyet seviyesi ile veri faydası arasında denge kurmayı sağlayan fayda temelli yaklaşımdır. Genelleştirme, baskılama, anatomi ve pertürbasyon gibi çeşitli operatörlerden yararlanarak paylaşılan veriyi ifşa saldırılarına karşı korur [21, 22]. Paylaşılan veriler genellikle mikro veri formatında olup, satırlar kayıtları sütunlar ise öznitelikleri temsil eder [23]. Bu öznitelikler tam-tanımlayıcı, yarı-tanımlayıcı, hassas ve hassas-olmayan olmak üzere dört farklı sınıfta değerlendirilir [24]. Tam-tanımlayıcılar; TC kimlik no, ad-soyad, pasaport numarası vb. gibi kişiyi doğrudan tanımlayan bilgilerdir. Doğrudan tanımlama özelliği olmasa da çeşitli özniteliklerin bir araya gelmesiyle oluşan ve veri sahibinin kimliğini tanımlayabilme potansiyeline sahip öznitelik grubuna ise yarı-tanımlayıcılar denir. Yaş, cinsiyet ve posta kodu özniteliklerinin bir araya gelmesiyle oluşturduğu grup yarı-tanımlayıcılara örnek olarak verilebilir. Hastalık, etnik köken ve maaş gibi kişinin mahrem bilgisi olarak nitelendirilen bilgiler ise hassas özniteliklere birer örnektir. Herhangi bir ifşa potansiyeli öngörülmeyen öznitelikler de hassas olmayan öznitelikler olarak sınıflandırılır.

Literatürde, anonimleştirme yaklaşımını uygulayan çeşitli mahremiyet koruma modelleri mevcuttur. k-Anonimlik, l-Çeşitlilik, t-Yakınlık ve δ-Mevcudiyet en yaygın kullanılan modellerden olup aşağıda kısaca açıklanmıştır.

k-Anonimlik: kayıt kümesi içerisindeki her bir kaydın tekil birer kişiye ait olduğu kabul edilerek, bir kaydın en az k-1 tane kayıttan ayırt edilememesini sağlar. Bu model sayesinde saldırgan, bir kurbanın yarı-tanımlayıcılarının değerini bilse bile o kurbanı ancak 1/k oranında ifşa edilme ihtimaline sahip olur [25]. Kimlik saldırısına karşı geliştirilmiş bir modeldir. k-Anonimliğin NP-Zor bir problem olduğu [26] çalışmasında ispatlanmıştır.

l-Çeşitlilik: k-Anonimlik modeli sadece yarı-tanımlayıcıları dikkate aldığı için hassas öznitelik ifşasına karşı koruma sağlayamaz. Bu sorunu gidermek adına, hassas özniteliklerin mahremiyetini koruyan l-Çeşitlilik modeli [2] çalışmasında önerilmiştir. Bu model, her bir eşlenik sınıfta en az l adet farklı hassas bilginin tutulmasını sağlayarak hassas öznitelik ifşasını engeller.

t-Yakınlık: l-Çeşitlilik, bir eşlenik sınıf içerisindeki hassas bilgilerin dağılımının genel dağılımdan önemli ölçüde farklı olması durumunda ortaya çıkabilecek çarpıklık saldırısına karşı koruma sağlayamaz. t-Yakınlık bu sorunu giderme adına önerilen ve bir eşlenik sınıf içerisindeki hassas bilgilerin dağılımının veri kümesindeki tüm dağılımına t değeri kadar yakın olmasını sağlayan bir mahremiyet koruma modelidir [27, 28].

δ-Mevcudiyet: arka plan bilgisine sahip saldırganın yayınlanan veri kümesinde kurbanın olup olmadığını bilmesi, bir üyelik çıkarımı yapmasını sağlar. Üyelik ve arka plan bilgisine sahip olan saldırgan veri bağlama yöntemleriyle kurbanın kimliğini belirleyebilir. Üyelik bilgisinin keşfini zorlaştırmak amacıyla δ-Mevcudiyet modeli [19] numaralı çalışmada önerilmiştir. Yayınlanan veri kümesini, saldırganın arka plan bilgisini temsil eden genel bir veri kümesinin alt kümesi olarak modeller. OAN modelinde mahremiyet riskini belirli seviyede tutmak

amacıyla, literatürde yaygın olarak kullanılan ve uygulanma maliyeti düşük olan k-Anonimlik modelinden faydalanılmıştır. OAN modeli, mahremiyet seviyesini düşürmeden veri faydasını arttırmayı ön plana çıkardığı için, mahremiyetin k-Anonimlik düzeyinde korunması önemli olacaktır. k-Anonimlik modelini uygulayan ve literatürde sıklıkla kullanılan bazı algoritmalar sonraki bölümde açıklanmıştır.

4. ANONİMLEŞTİRME ALGORİTMALARI (ANONYMIZATION ALGORITHMS)

Anonimleştirme zor bir problem olduğu için bu problemi çözmek adına literatürde çok sayıda algoritma geliştirilmiştir. Bu algoritmalar genel olarak optimallik, işlediği veri boyutu sayısı, işlem yönü ve veriyi bölme stratejisine göre çeşitlilik gösterir. Bu algoritmalardan, literatürde sıklıkla kullanılanları aşağıda kısaca açıklanmış, karşılaştırılmış ve hangi algoritmanın neden seçildiği belirtilmiştir.

MinGen: tüm k-Anonim genelleştirmelerini sorgular. Genelleştirme ve baskılama operatörlerini kullanır. Optimal çözümü arayan bir algoritma olup tek boyutlu veri anonimleştirmesini destekler. Ancak yüksek boyutlu ve geniş veri kümeleri için uygun bir algoritma değildir [29].
Incognito: tüm k-Anonim genelleştirmelerini sorgular. Optimal bir algoritma olup, tek boyutlu veri anonimleştirmesi yapar. Genelleştirme ve baskılama operatörlerini kullanır. Yüksek boyutlu ve geniş veri kümeleri için uygun bir çözüm değildir [30].

Flash: k-Anonimliği sağlayan optimal bir algoritmadır. Tam genelleştirme kafesinde aşağıdan yukarıya dolaşarak kafeste yollar oluşturur ve bu yolları k-Anonimliği sağlama adına kontrol eder. Optimal çözümü bulmaya çalıştığı için yüksek boyutlu ve geniş veri kümleri için uygun bir çözüm değildir [31]. Datafly: geniş veri kümelerinde k-Anonimliği sağlamak için geliştirilen ilk algoritmadır. Yarı-tanımlayıcı grubunun büyüklüğü kadar bir dizi üretir ve dizi elemanlarının kombinasyonları k adet tekrarlamadan daha az olacak şekilde veriyi aç-gözlü bir yaklaşımla genelleştirir. Genelleştirme ve baskılama operatörlerini kullanır. Optimale yakın bir çözüm sunduğu için yüksek boyutlu ve geniş veri kümelerinde uygun çözümler üretebilir [32].

Bottom-up Generalization: minimal k-Anonimliği sağlamak için geliştirilen optimale yakın bir çözümdür. Algoritma, orijinal veride k-Anonimliği ihlal eden veriden başlar ve her bir aşamada arama metriğine dayanarak genelleştirme yapar. Sorgulanan veri eğer bir üst seviyeye genelleştirilecek ise aynı ağaçta ve seviyedeki diğer veriler de bir üst seviyeye genelleştirilir. Alt-ağaç genelleştirmesi ve baskılama operatörlerini kullanır [33].

Top-down Specialization: en üst seviyede genelleştirilmiş verilerin aşağı yönde özelleştirilmesiyle anonimleştirmeyi sağlar. k-Anonimliği ihlal eden herhangi bir özelleştirme kalmayana kadar süreç devam eder. Alt-ağaç genelleştirmesi ve baskılama operatörlerinden yararlanan optimale yakın bir çözümdür [34]. Mondrian: minimal k-Anonimliği bulmaya yarayan optimale yakın bir algoritmadır. Belirli bir yarı-tanımlayıcı grubu içerisinde tek değer özelleştirmesi yapar. Bu özelliğinden dolayı diğer algoritmalara göre daha kaliteli bir veri sunar. Optimale yakınsama faktörünün ve çalışma zamanının diğer algoritmalara kıyasla daha iyi olmasından dolayı literatürde en çok tercih edilen algoritmalardan biridir. Çok boyutlu genelleştirme operatörünü kullanır [35].

Yukarıda belirtilen anonimleştirme algoritmaları Tablo 1'de karşılaştırılmıştır. Bu karşılaştırma sonucunda, OAN modeli için en uygun algoritmanın Mondrian olduğuna karar verilmiş ve bunun gerekçeleri aşağıda sunulmuştur;

- Optimale yakın bir çözüm sunarak kabul edilebilir bir çözüm üretmesi,
- Çok boyutlu veri anonimleştirmesi yaptığından dolayı günümüz ihtiyaçlarına yönelik olması,
- Parçalı bölme stratejisini kullanarak öznitelik uzayını daha etkin bölmesi,
- Çok boyutlu genelleştirme işlemini kullanarak veri kaybını azaltması ve
- Hiyerarşi tabanlı olmamasıdır.

Mondrian algoritmasının daha iyi anlaşılması için algoritmanın nasıl çalıştığı Şekil 2'de gösterilmektedir. Algoritmada öncelikle öznitelik uzayını bölmek için bir boyut seçilir. Seçilen boyuttaki verilerin frekansı hesaplanır ve bölme noktası olarak ortanca değeri alınır. Bu değerden küçük ve eşitleri sol kümeye, büyükleri ise sağ kümeye atanır. Bu işlem bölünecek veri kalmadığı müddetçe devam eder. En sonunda her bir parça kendi içerisinde genelleştirilerek anonim veri kümesi elde edilir. Optimale yakın bir çözüm sunan Mondrian algoritmasının O(nlogn) zaman karmaşıklığına sahip olduğunu belirtmekte fayda vardır.

Tablo 1. Anonimleştirme algoritmalarının karşılaştırılması (Comparision of some anonymization algorithms)

Algoritma	Optimallik	Boyut	İşlem Yönü	Bölme Stratejisi
MinGen [29]	Optimal	Tekli	Aşağıdan-yukarıya	Hiyerarşik
Incognito [30]	Optimal	Tekli	Aşağıdan-yukarıya	Hiyerarşik
Flash [31]	Optimal	Tekli	Aşağıdan-yukarıya	Hiyerarşik
Datafly [32]	Yakın Optimal	Tekli	Aşağıdan-yukarıya	Hiyerarşik
Bottom-up G. [33]	Yakın Optimal	Tekli	Aşağıdan-yukarıya	Hiyerarşik
Top-down S. [34]	Yakın Optimal	Tekli	Yukarıdan-aşağıya	Hiyerarşik
Mondrian [35]	Yakın Optimal	Çoklu	Yukarıdan-aşağıya	Parçalı

Algoritma-1: Mondrian algoritması

```
1  fonksiyon Anonimleştir(S):
2      Girdi: S kayıtlar kümesi
3      Çıktı: S' anonim kayıtlar kümesi
4      eğer S bölünemezse
5          S'i genelleştirerek döndür
6      aksi halde
7          dim ← bölünecek_boyutu_seç(S)
8          fs  ← frekans_hesapla(S, dim)
9          sv  ← ortanca_bul(fs)
10         L   ← {s ∈ S : s.dim ≤ sv}
11         R   ← {s ∈ S : s.dim > sv}
12     döndür Anonimleştir(R) U Anonimleştir(L)
```

Şekil 2. Mondrian Algoritması (Mondrian Algorithm) [35]

Anonimleştirme algoritmaları ile mahremiyet problemine belirli seviyelerde çözüm sunulurken, üretilen anonim verinin kalitesini ölçmek için de çeşitli metriklere ihtiyaç duyulur. Bilgi kaybı metriği (ILoss) [36], en az bozulma metriği (MD) [37], eşlenik sınıflar ortalaması (AECS) [35], ve ayırt edilebilirlik metriği (DM) [38] veri kalitesini ölçmede kullanılan genel amaçlı metriklerden bazılarıdır. Bu metriklerden AECS ve DM, eşlenik sınıflarını dikkate alır. Bu çalışmada, kullanılan Mondrian algoritması eşlenik sınıfları dikkate aldığı için AECS ve DM metrikleri bu çalışmada tercih edilmiş ve aşağıda kısaca açıklanmıştır.

AECS: ortalama eşlenik sınıf büyüklüğünü ölçer [35]. Bu metriğin küçük değerleri için daha az elemandan oluşan eşlenik sınıflar ortaya çıkar ve böylece eşlenik sınıf sayısı artarak fayda artmış olur. $|T|$ bir T tablosundaki kayıt sayısını, EC eşlenik sınıfı, $|EC_S|$ eşlenik sınıflar kümesindeki eşlenik sınıf sayısını ve k ise k-anonimlik parametresini göstermek üzere, bu metriğe ait formül Eş. 1'de sunulmuştur;

$$AECS(T) = \frac{|T|}{|EC_S| \times k} \quad (1)$$

DM: her bir kayda diğer kayıtlardan ayırt edilememesi durumu için bir ceza puanı atar [38]. Eğer bir kayıt, $|T[qid]|$ büyüklüğünde bir qid grubuna ait ise, bu kayıt için ceza değeri $|T[qid]|$ olur. qid gruba ait ceza ise $|T[qid]|^2$ olarak hesaplanır. Genelleştirilmiş bir T tablosuna ait tüm ceza puanı ise Eş. 2'deki gibi hesaplanır;

$$DM(T) = \sum_{qid_i} |T[qid_i]|^2 \quad (2)$$

5. OAN: AYKIRI KAYIT YÖNELİMLİ FAYDA TEMELLİ MAHREMİYET KORUMA MODELİ (OAN: OUTLIER RECORD-ORIENTED UTILITY-BASED PRIVACY PRESERVING MODEL)

Bu bölümde çalışma kapsamında önerilen OAN modeli tanıtılmış, içerdiği katmanlar açıklanmış, modele ve katmanlara ait algoritmalar verilmiş ve modelin akış şeması sunulmuştur.

5.1. OAN Anonimleştirme Modeli (OAN Anonymization Model)

OAN, aykırı verileri yöneterek veri faydasını arttıran ve hesaplama maliyetini düşüren yeni bir mahremiyet koruma modelidir. Geleneksel yaklaşımlardan farklı olarak, aykırı verileri anonimleştirme öncesi tespit ederek hesaplama maliyetini düşürmesi ve aykırı verilerin tamamını faydayı arttırıcı bir şekilde kullanması bu modelin öne çıkan yenilikleridir.

Önerilen modelde aykırı veri yönetimi iki aşamadan oluşur. İlk aşama, aykırı verilerin anonimleştirme öncesi tespit edilmesidir. Anonimleştirme zor bir problemdir. Her ne kadar optimal veya yaklaşık çözümler geliştirilse de anonimleştirilecek veri veya öznitelik sayısının artması arama uzayının büyümesine neden olur. Geleneksel aykırı veri yönetim yaklaşımları bu kapsamda değerlendirildiğinde, anonimleştirme sonrası veri kümesinden çıkarılacak bir verinin anonimleştirmeye dâhil edilmesi gereksiz bir hesaplama maliyeti oluşturur ve bunun sonucunda toplam hesaplama maliyeti artar. Ancak OAN modelinde, aykırı verilerin anonimleştirme öncesi tespit edilmesiyle hesaplama maliyeti düşürülür. İki ayrı alt kümeye ayrılan verilerden her kümenin kendi içerisinde anonimleştirilmesiyle arama uzayı küçültülerek hesaplama maliyeti düşürülmüş olur. OAN modelinin hesaplama maliyeti açısından değerlendirilmesinde, literatürde fayda temelli ilk model olan ρ-Gain kullanılmıştır. Her iki modelin aykırı veri yönetim yaklaşımları Şekil 3'de gösterilmiştir. Verilen bu şekilde, T kümesindeki veri sayısı N, aykırı veri kümesi ORS (Outlier Record Set)'deki veri sayısı O ve normal veri kümesi URS (Utility Record Set)'deki veri sayısı U ve N=O+U olsun. OAN modelindeki aykırı veri yönetim yaklaşımında, N sayıda eleman içeren veri kümesinin O ve U sayıda eleman içeren iki alt kümeye ayrıldığı kabul edilsin. Bu durumda, anonimleştirme aşamasındaki toplam arama uzayı büyüklüğü, c bir sabit değer olmak üzere, $c^O + c^U$ olur.

ρ-Gain modelindeki aykırı veri yönetim yaklaşımı ise anonimleştirme için c^N büyüklüğünde bir arama uzayı sunar. Bu durumda, $c^N > c^O + c^U$ olduğu için OAN modelinin diğer modele göre hesaplama maliyeti açısından daha etkin bir çözüm olduğu görülür.

İkinci aşama ise, aykırı verilerin tamamının faydayı arttıracak şekilde değerlendirilmesidir. Bu aşamada, aykırı veri kümesi yinelemeli olarak yeni alt kümelere ayrılır ve tüm alt kümelerin tamamı kullanılarak veri faydası arttırılır. Aykırı veri kümesinin parçalanması, bu verilerin kendi içerisinde daha iyi ayrıştırılmasını sağlayarak veri faydasına olumlu bir katkı sağlar. Aykırı verileri yeni alt kümelere ayırmak için, ρ-Gain modelinde kullanılan veri parçalama stratejisinden yararlanılmıştır. Şekil 4'de gösterilen bu stratejide, ilk önce aykırı veriler tespit edilir. Sonra tüm veri kümesi, normal veri kümesi (URS_1) ve aykırı veri kümesi (ORS_1) olarak ikiye ayrılır. Devamında, ORS_1 içerisindeki aykırı veriler tespit edilir ve bu küme yeni URS_2 ve ORS_2 alt kümelerine ayrılır. Bu işlem yinelemeli olarak belirli bir şart sağlanana kadar devam eder.

Şekil 5'de, önerilen OAN modeline ait algoritma verilmiştir. Algoritmada gerçekleştirilen işlemler 5 farklı katmanlı bir yapı ile yapılmıştır. Hazırlık katmanında ham veri kümesi işlenmeye hazır hale getirilir. Aykırı veri tespit katmanında aykırı veriler tespit edilerek URS ve ORS kümeleri oluşturulur. Anonimleştirme katmanında URS ve ORS ayrı ayrı anonimleştirilir. Değerlendirme katmanlarında ise durdurma kriterinin sağlanıp sağlanmadığı kontrol edilir. Son olarak da anonim hale gelen veri kümesi Yayınlama katmanında yayınlanır.

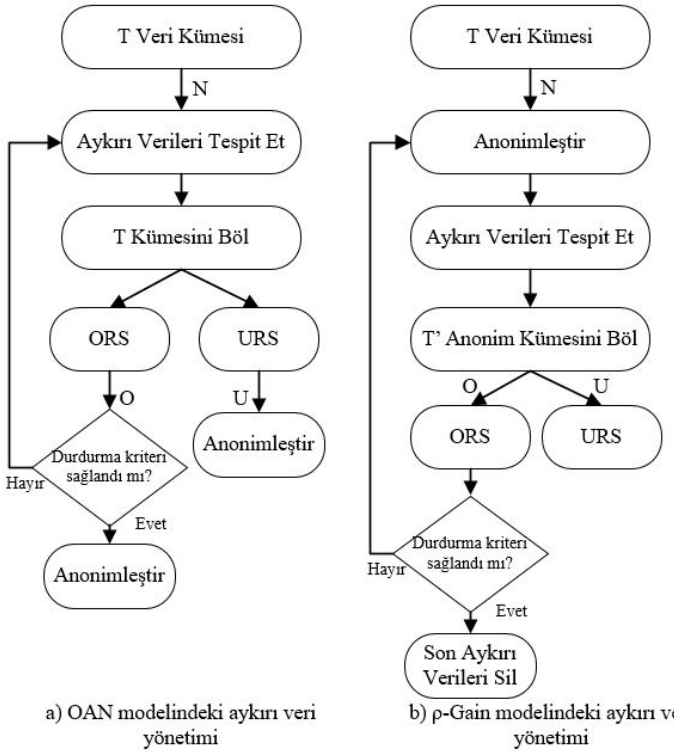
Şekil 5'de algoritması verilen OAN modelindeki toplam veri faydası Eş. 3'deki formüle göre hesaplanır. Ayrıca AECS metriği kullanılması durumunda toplam veri faydası Eş. 4'deki gibi de hesaplanabilir.

$$DM_T = \sum_{i=1}^{N} DM(URS_i) + DM(ORS_N) \quad (3)$$

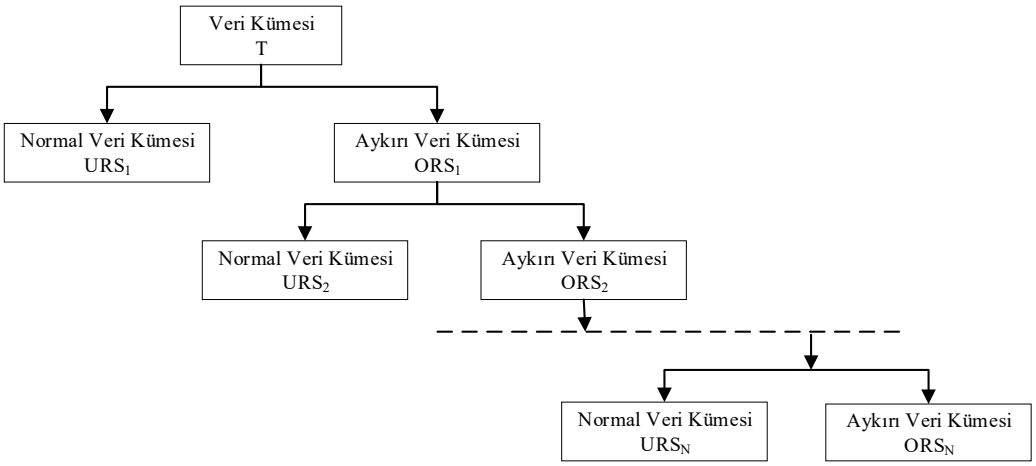
$$AECS_T = \sum_{i=1}^{N} AECS(URS_i) + AECS(ORS_N) \quad (4)$$

OAN modeline ait akış şeması Şekil 6'da gösterilmekte olup, her adım sırasıyla aşağıda açıklanmıştır.

- T veri kümesi modele girdi olarak verilir.
- Ön işlem aşamasında öznitelik sınıfları ve durdurma kriteri belirlenir, veri kümesi normalize edilir ve S veri kümesi elde edilir (bu çalışmada durdurma kriterinin belirlenmesi için DM metriği kullanılmıştır).
- Başlangıç parametresi olarak k değeri belirlenir (bu çalışmada k=10 alınmıştır).
- $DM(S^A)$ değerine başlangıçta N^2 değeri atanır.
- S veri kümesindeki aykırı verilerin belirlenmesi için LOF değerleri hesaplanır.
- LOF(S) değerine göre her iterasyonda bir t eşik değeri belirlenir.
- t eşik değerine göre aykırı veriler belirlenir.
- Belirlenen t eşik değeri ile veri kümesi URS_i ve ORS_i olarak ikiye bölünür.
- ORS_i ve URS_i ayrı ayrı anonimleştirilerek ORS_i^A ve URS_i^A anonim veri kümeleri elde edilir ve mevcut fayda kümesi P oluşturulur.



Şekil 3. Aykırı veri yönetim yaklaşımları (Outlier management approaches)



Şekil 4. ρ-Gain modelinin veri kümesi parçalama stratejisi (Record set partitioning strategy of ρ-Gain)

Algoritma-2: OAN algoritması		**Katmanlar**
1	**Girdi:** T veri kümesi, k anonimlik değeri	
2	**Çıktı:** T^A anonim veri kümesi	
3	URS, ORS, URS^A, ORS^A, P ← Ø	
4	$DM(S^A) \leftarrow N^2$	
5	S ← Veriyi_hazırla(T)	*Hazırlık*
6	**fonksiyon** OAN (S_i):	
7	(URS_i, ORS_i) ← Aykırı_verileri_bul(S_i)	*Aykırı Veri Tespiti*
8	URS_i^A ← Anonimleştir(URS_i)	*Anonimleştirme*
9	ORS_i^A ← Anonimleştir(ORS_i)	*Anonimleştirme*
10	$P_i \leftarrow P_i \cup URS_i^A$	
11	**eğer** $DM(S_i^A) \geq DM(URS_i^A) + DM(ORS_i^A)$	*Değerlendirme-1*
12	$S_i \leftarrow ORS_i$	
13	$S_i^A \leftarrow ORS_i^A$	
14	**döndür** OAN (S_i)	
15	**aksi halde**	*Değerlendirme-2*
16	**eğer** i=1	
17	**döndür** Yayınla(S_i^A)	*Yayınlama-1*
18	**aksi halde**	
19	**döndür** Yayınla($ORS_{i-1}^A \cup P_{i-1}$)	*Yayınlama-2*

Şekil 5. OAN algoritması ve ilgili katmanları (Algorithm of OAN and related layers)

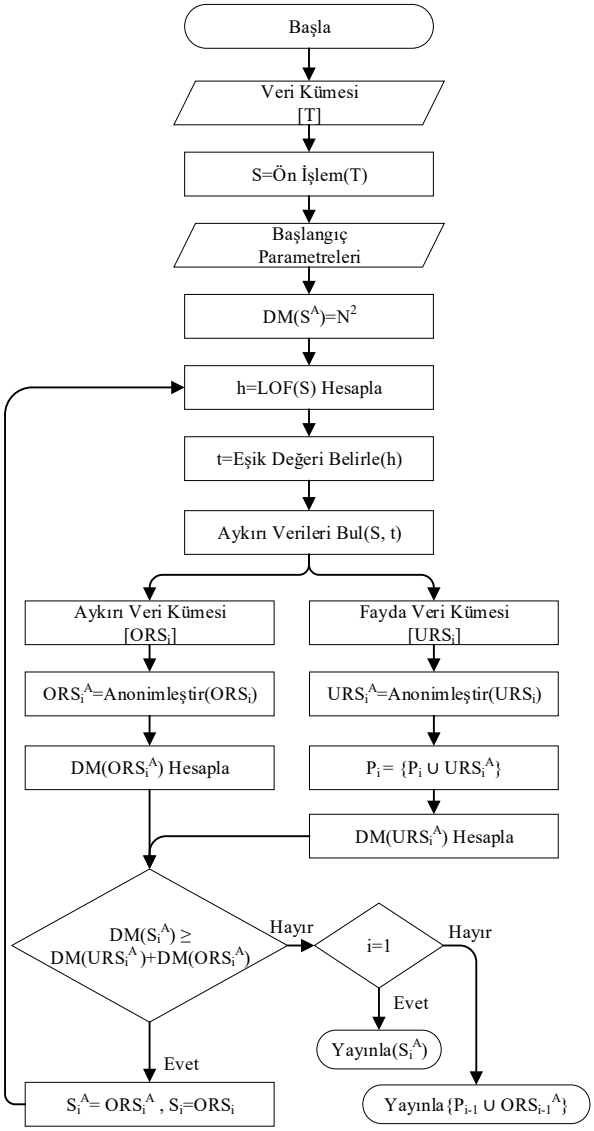
- Eğer $DM(S_i^A) \geq DM(URS_i^A) + DM(ORS_i^A)$ şartı sağlanırsa veri kümesi S_i=ORS_i, mevcut anonim aykırı veri kümesi S_i^A=ORS_i^A olur ve yineleme devam eder.
- Eğer yukarıda belirlenen şart sağlanmazsa, veri kümesi iki farklı stratejiye göre yayınlanır.

5.2. Katmanların İncelenmesi (Examination of the Layers)

OAN modeli beş katmanlı bir yapıya sahip olup bu katmanlar aşağıda açıklanmıştır.

Hazırlık Katmanı: özniteliklerin sınıflandırılması, veri kümesinin normalizasyonu, k değerinin ve durdurma kriterinin belirlenmesi bu katmanda gerçekleştirilir. Bu katmanda yapılan işlemler aşağıda açıklanmış ve algoritması Şekil 7'de sunulmuştur.

- Özniteliklerin sınıflandırılması: özniteliklerin tam-tanımlayıcı, yarı-tanımlayıcı, hassas ve hassas olmayan olmak üzere sınıflandırılmasıdır. Önerilen model, k-anonimliği uyguladığı için bu aşamada yarı-tanımlayıcıları belirlenmektedir.
- Veri normalizasyonu: farklı değer aralıklarına sahip özniteliklerin standart haline getirilmesi işlemidir. Çeşitli normalizasyon teknikleri bu aşamada kullanılabilir.
- k değerinin belirlenmesi: mahremiyet seviyesinin belirlendiği aşamadır. Bu çalışmada k-anonimlik uygulandığı için k parametresinin belirlenmesi gerekmektedir.
- Durdurma kriterinin belirlenmesi: iterasyon sayısı, çeşitli metrik değerleri veya farklı parametreler durdurma kriteri olabilir. Bu çalışmada durdurma kriteri olarak DM metrik değeri seçilmiştir.



Şekil 6. Önerilen OAN modelinin akış şeması
(Flowchart of the proposed OAN model)

Aykırı Veri Tespit Katmanı: önerilen modelin aykırı veri yönetim yaklaşımını içeren katmanıdır. Aykırı veri tespiti üzerine literatürde istatistik, uzaklık, yoğunluk ve kümeleme tabanlı gibi çeşitli yaklaşımlar mevcuttur [39-41]. Bu katmanda yoğunluk tabanlı yaklaşımlardan LOF algoritması kullanılmıştır. LOF algoritması veri kümesindeki her bir veriye bir aykırılık değeri atar. Atanan bu değerlere göre belirli bir eşik değerinden büyük olan veriler aykırı, diğerleri ise normal veri olarak kabul edilir. Şekil 8'de bu katmana ait algoritma gösterilmektedir.

Anonimleştirme Katmanı: normal ve aykırı veri kümelerinin anonimleştirildiği katmandır. Anonimleştirme, k-Anonimlik mahremiyet modeli kullanılarak gerçekleştirilmekte ve bunun için de Mondrian algoritmasında faydalanılmaktadır. Bu katmanda Mondrian algoritması haricinde diğer anonimleştirme algoritmaları da tercih edilebilir. Şekil 9'da bu katmana ait algoritma gösterilmektedir.

Algoritma-3: Hazırlık katmanı algoritması	
1	**Girdi:** T veri kümesi
2	**Çıktı:** S işlenmeye hazır veri kümesi
3	**fonksiyon** Veriyi_hazırla(T)
4	R ← Öznitelikleri_sınıflandır(T)
5	S ← Normalize_et(R)
6	k ← k_belirle()
7	Durdurma_kriteri_belirle()
8	**döndür** S

Şekil 7. Hazırlık katmanı algoritması
(Algorithm of preparation layer)

Algoritma-4: Aykırı veri tespit katmanı algoritması	
1	**Girdi:** S veri tablosu
2	**Çıktı:** URS, ORS
3	**fonksiyon** Aykırı_verileri_bul (S)
4	A ← LOF(S)
5	t ← Eşik_değeri_belirle(A)
6	(URS, ORS) ← Veriyi_ikiye_bol(S, t)
7	**döndür** (URS, ORS)

Şekil 8. Aykırı veri tespit katmanı algoritması
(Algorithm of outlier detection layer)

Algoritma-5: Anonimleştirme katmanı algoritması	
1	**Girdi:** E kayıt kümesi
2	**Çıktı:** k-anonim E^A veri kümesi
3	**fonksiyon** Anonimleştir(E)
4	E^A ← Mondrian(E)
5	**döndür** (E^A)

Şekil 9. Anonimleştirme katmanı algoritması
(Algorithm of anonymization layer)

Değerlendirme Katmanı: bir durdurma kriterine bağlı olarak aykırı veri tespiti, anonimleştirme ve yayınlama katmanlarının çalışmasını veya durmasını sağlayan alt aşamaları içerir. Belirlenen durdurma kriteri sağlanırsa sırasıyla diğer katmanlara gidilir aksi halde algoritma sonlanarak yayınlama katmanına gidilir. Şekil 10'da bu katmana ait algoritma gösterilmektedir.

Yayınlama Katmanı: faydası arttırılmış olan anonim verinin yayınlandığı son katmandır. Bu katmana gelen veri mevcut duruma göre ya birleştirerek yada olduğu gibi yayınlar. Şekil 11'de bu katmana ait algoritmanın kodu gösterilmektedir.

Algoritma-6: Değerlendirme katmanı algoritması	
1	**Girdi:** S_i^A, URS_i^A, ORS_i^A
2	**Çıktı:** yok
3	Aşama-1
4	**eğer** $DM(S_i^A) \geq DM(URS_i^A) + DM(ORS_i^A)$
5	**devam et**
6	Aşama-2
7	**aksi halde**
8	Yayınlama katmanına **git**

Şekil 10. Değerlendirme katmanı algoritması
(Algorithm of evaluation layer)

Algoritma-7: Yayınlama katmanı algoritması	
1	**Girdi:** P, ORS^A veya S^A
2	**Çıktı:** T^A anonim veri kümesi
3	**fonksiyon** Yayınla
4	$T^A \leftarrow P \cup ORS^A$
5	veya
6	$T^A \leftarrow S^A$
7	**döndür** T^A

Şekil 11. Yayınlama katmanı algoritması
(Algorithm of publishing layer)

6. DENEYSEL ÇALIŞMALAR
(EXPERIMENTAL STUDIES)

Bu bölümde, kullanılan veri kümesi tanıtılmış, gerçekleştirilen deneyler ve elde edilen sonuçlar sunulmuştur. Önerilen modeli doğrulamak ve test etmek için yapılan deneylerde Intel Core i3-6100 2.3 GHz işlemci ve 4 GB ram özelliğine sahip bilgisayar kullanılmıştır.

Literatürdeki anonimleştirme çalışmalarında defakto-standart olarak kullanılan ADULT [42] veri kümesi bu çalışmada tercih edilmiştir. ADULT veri kümesi içerisinde bulunan 18680 adet eksik veri, veri kümesinden çıkarılmıştır. Bu veri kümesi hakkında özet bilgi Tablo 2'de sunulmuştur. Yapılan deneylerde yarı-tanımlayıcı olarak seçilen öznitelikler ise yaş, kilo, gelir bilgisi, gider bilgisi ve haftalık çalışma saati olarak seçilmiştir.

Deneylerde ADULT veri kümesi OAN anonimleştirme modeli kullanılarak 10-anonim hale getirilmiştir. LOF eşik değeri belirlemede literatürde standart bir yaklaşım olmadığı için bu çalışmada LOF değerlerinin ortalaması alınmıştır. Deneyde her iterasyonda seçilen LOF değerlerine göre elde edilen aykırı ve normal veri sayıları ve bunların DM metrik değerleri Tablo 3'de gösterilmiştir.

Tablo 2. ADULT veri kümesi özet bilgisi
(Metadata of ADULT data)

Özellik	Açıklama
Kayıt sayısı	48842
Öznitelik sayısı	14
Sınıf sayısı	2
Öznitelik karakteristiği	Kategorik ve nümerik
Eksik veri içeren kayıt sayısı	18680
Eksik veri içermeyen kayıt sayısı	30162

Tablo 3'de başlangıç iterasyonu, tüm veri kümesinin klasik Mondrian algoritması kullanılarak anonimleştirilmesi durumunda elde edilen DM değerini göstermektedir. Her iterasyon için, eğer $DM(ORS_i) > DM(ORS_{i+1}) + DM(URS_{i+1})$ şartı sağlanırsa veri faydasının arttığı, diğer durumlarda ise algoritmanın sonlanarak modelin çalışmasının durduğu kabul edilmektedir. İterasyon 1-3 arası önerilen model ile veri faydasının arttırıldığı ancak iterasyon 3 sonrası algoritmanın durduğu gözlemlenmiştir. Bu deneyde sarı, turuncu ve mavi ikililerden her bir renk içerisindeki ilk değer aynı renkli ikinci değerden büyüktür. Yani, iterasyon 1'de 412888<423654, iterasyon 2'de 119359 <121529 ve iterasyon 3'de ise 32057<32395 olduğu görülmektedir. Ancak iterasyon 3'de durdurma kriteri sağlanmış ve algoritma sonlanarak anonim veri kümesini yayınlamıştır. Modelin sunduğu toplam fayda DM metriği açısından, Eş.3'deki formülden yararlanarak, DM_T=410380 olarak elde edilir.

Tablo 4'de ise deney sonucunda elde edilen eşlenik sınıf sayıları (ES) gösterilmiştir. Her iterasyon için, eğer $ES(ORS_i) < ES(ORS_{i+1}) + ES(URS_{i+1})$ şartı sağlanırsa veri faydasının arttığı, diğer durumlarda ise algoritmanın sonlanarak modelin çalışmasının durduğu kabul edilmektedir. İterasyon 1-3 arası önerilen modelin veri faydasını arttırdığı ancak iterasyon 3 sonrası algoritmanın durduğu gözlemlenmiştir. Bu deneyde sarı, turuncu ve mavi ikililerden her bir renk içerisindeki ilk değer aynı renkli ikinci değerden küçüktür. Yani, iterasyon 1'de 2324>2261, iterasyon 2'de 670>661 ve iterasyon 3'de ise 196 >192 olduğu görülmektedir. Ancak iterasyon 3 sonrası durdurma kriteri sağlanmış ve algoritma sonlanarak anonim veri kümesini yayınlamıştır. Modelin sunduğu toplam veri faydası ES değeri açısından, ES_T=2337 olarak elde edilmiştir.

Şekil 12.a'da DM değerleri, Şekil 12.b'de ise ES değerleri kullanılarak hesaplanan AECS değerlerindeki değişim gösterilmektedir. Her iki metrik için, iterasyon 0'da veriye klasik Mondrian algoritmasının uygulanması sonrası edilen veri faydası, iterasyon 1, 2 ve 3'de ise OAN modelinin uygulanması ile elde edilen veri faydası gösterilmektedir. Bu sonuçlar, önerilen OAN modelinin doğruluğunu ve veri faydasını arttırmadaki başarısını ortaya koymaktadır.

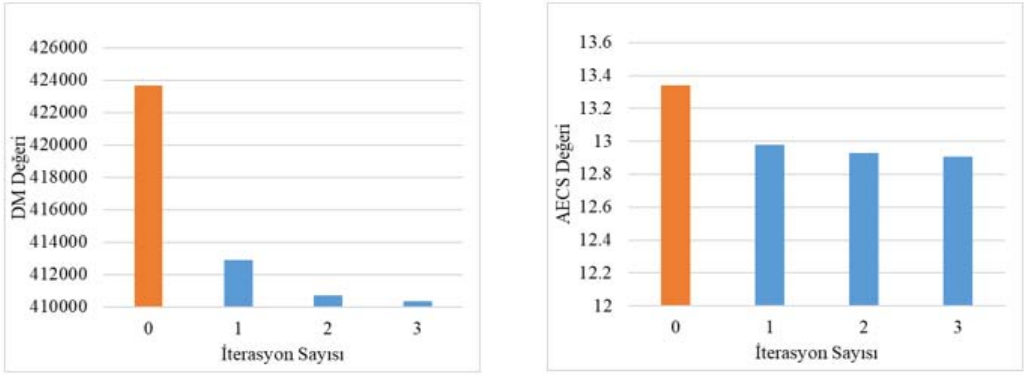
Yapılan deneyler neticesinde, veri kümesinin klasik anonimleştirme işlemi sonrası sunduğu veri faydasının, önerilen model ile belirli bir seviyede arttığı gözlemlenmiştir. Bu durum, önerilen OAN modelinin veri

Tablo 3. DM metrik sonuçları (Results of DM metric)

İterasyon No	İşlenen Veri Sayısı	LOF Değeri	|URS|	DM(URS)	|ORS|	DM(ORS)	DM(URS)+ DM(ORS)
başlangıç	30162	-	-	-	30162	423654	423654
1	30162	1.146	21469	291359	8693	121529	412888
2	8693	1.121	6280	86964	2413	32395	119359
3	2413	1.376	1664	22292	749	9765	32057
DM_0=423654, DM_T=410380							

Tablo 4. ES sonuçları (Results of ES)

İterasyon No	ES(URS)	ES(ORS)	ES(URS) + ES(ORS)
başlangıç	-	2261	2261
1	1663	661	2324
2	478	192	670
3	136	60	196
ES_0=2261, ES_T=2337			



a) DM metrik sonuçları b) AECS metriklerinin sonuçları

Şekil 12. OAN modelinin uygulanmasıyla elde edilen metrik sonuçları (The metric results of OAN)

faydasını arttırmada başarılı olduğunu göstermektedir. Ayrıca OAN modelinde uygulanan aykırı veri yönetim yaklaşımının fayda temelli başka bir model olan ρ-Gain'e kıyasla daha maliyet-etkin bir çözüm olduğu beşinci bölümde gösterilmiştir.

7. SONUÇLAR (RESULTS)

Bu çalışmada, aykırı verilerden elde edilecek faydayı arttırmayı ve hesaplama maliyetini etkin kılmayı amaçlayan fayda temelli yeni bir anonimleştirme modeli önerilmiştir. Önerilen modelde tüm aykırı veriler kullanılarak toplam veri faydası arttırılmış ve aykırı veriler anonimleştirme öncesi tespit edilerek maliyet açısından etkin bir model oluşturulmuştur. Aykırı verilerin yoğunluk tabanlı bir yaklaşımla tespit edilmesi ilk defa bu modelde uygulanmıştır. Deneysel çalışmalarda elde edilen sonuçlar önerilen OAN modelinin veri faydasını arttırmada başarılı olduğunu göstermiştir.

Gelecek çalışmalarda, LOF eşik değeri belirlemede, aykırı veri tespitinde ve anonimleştirmede farklı algoritma, yöntem ve yaklaşımların kullanılabileceği ve farklı k değerleri için önerilen modelin test edilebileceği değerlendirilmektedir.

KAYNAKLAR (REFERENCES)

1. Sweeney L. Simple demographics often identify people uniquely. https://dataprivacylab.org. Yayın tarihi 2000. Erişim tarihi Mart 19, 2018.
2. Machanavajjhala A., Gehrke J., Kifer D., Venkitasubramaniam M., l-diversity: Privacy beyond k-anonymity, IEEE International Conference on Data Engineering, Atlanta-ABD, 24-24, 3-8 Nisan, 2006.
3. Motwani R., Nabar S.U., Anonymizing unstructured data, arXiv:0810.5582, 2008.
4. Fung B.C.M, Wang K., Fu A.W., Yu P.S., Introduction to Privacy-preserving Data Publishing: Concepts and Techniques, CRC Press, 2010.
5. Majeed A., Attribute-centric Anonymization Scheme for Improving User Privacy and Utility of Publishing e-health Data, Journal of King Saud University-Computer and Information Sciences, basımda, 2018.
6. Ramana K.V., Kumari V.V., Raju K., Impact of Outliers on Anonymized Categorical Data, International Conference on Advances in Digital Image Processing and Information Technology, Tirunelveli-Hindistan, 326-335, 23-25 Eylül, 2011.
7. Wang H.W., Liu R., Hiding Distinguished Ones into Crowd: Privacy-preserving Publishing Data with Outliers, International Conference on Extending Database Technology: Advances in Database Technology, Saint-Petersburg-Russian, 624-635, 23-26 Mart, 2009.
8. Wang H.W., Liu R., Hiding Outliers into Crowd: Privacy-preserving Data Publishing with Outliers, Data & Knowledge Engineering, 100, 94-115, 2015.
9. Vural Y., ρ-Kazanım: Mahremiyet Korumalı Fayda Temelli Veri Yayınlama Modeli, Doktora Tezi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2017.
10. Vural Y., Aydos M., A New Approach to Utility-Based Privacy Preserving in Data Publishing, IEEE International Conference on Computer and Information Technology, Dakka-Bangladeş, 204-209, 22-24 Aralık, 2017.
11. Vural Y., Aydos M., ρ-Gain: Utility Based Data Publishing Model, Journal of the Faculty of Engineering

and Architecture of Gazi University, 33(4), 1355-1368, 2018.

12. Lee H., Kim S., Kim J.W., Chung Y.D., Utility-preserving Anonymization for Health Data Publishing. BMC Medical Informatics and Decision Making, 17(1), 104-116, 2017.

13. Breunig M.M., Kriegel H., Ng R.T., Sander J., LOF: Identifying Density-based Local Outliers, ACM International Conference on Management of Data, Teksas-ABD, 93-104, 16-18 Mayıs, 2000.

14. Fung B.C.M, Wang K., Chen R., Yu P.S, Privacy-preserving Data Publishing: A Survey of Recent Developments, ACM Computing Surveys, 42(4), 1-53, 2010.

15. Wong R.C., Fu A.W., Wang K., Pei J., Minimality Attack in Privacy Preserving Data Publishing, International Conference on Very Large Databases, Viyana-Avusturya, 543-554, 23-23 Eylül, 2007.

16. Duncan G., Lambert D., The Risk of Disclosure for Microdata, Journal of Business & Economic Statistics, 7(2), 207-217, 1989.

17. Chen B., LeFevre K., Ramakrishnan R., Privacy Skyline: Privacy with Multidimensional Adversarial Knowledge, International Conference on Very Large Databases, Viyana-Avusturya, 543-554, 23-27 Eylül, 2007.

18. Sweeney L., Computational Disclosure Control: A Primer on Data Privacy Protection, Doktora Tezi, Massachusetts Institute of Technology, Deptartment of Electrical Engineering and Computer Science, Massachusetts, 2001.

19. Nergiz M.E., Atzori M., Clifton C., Hiding the Presence of Individuals from Shared Databases, ACM International Conference on Management of Data, Beijing-Çin, 665-676, 11-14 Haziran, 2007.

20. Fang W., Wen X.Z., Zheng Y., Zhou M., A Survey of Big Data Security and Privacy Preserving, IETE Technical Review, 34(5), 544-560, 2017.

21. Xu Y., Ma T., Tang M., Tian W., A Survey of Privacy Preserving Data Publishing Using Generalization and Suppression, Applied Mathematics & Information Sciences, 8(3), 1103-1116, 2014.

22. Ye Y., Wang L., Han J., Qiu S., Luo F., An Anonymization Method Combining Anatomy and Permutation for Protecting Privacy in Microdata with Multiple Sensitive Attributes, IEEE International Conference on Machine Learning and Cybernetics, Ningbo-Çin, 404-411, 9-12 Haziran, 2017.

23. Rahimi M., Bateni M., Mohammadinejad H., Extended k-anonymity Model for Privacy Preserving on Micro Data, International Journal of Computer Network and Information Security, 7(12), 42-51, 2015.

24. Lin W., Yang D., Wang J., Privacy Preserving Data Anonymization of Spontaneous ADE Reporting System Dataset, BMC Medical Informatics and Decision Making, 16(1), 21-35, 2016.

25. Sweeney L., k-anonymity: A Model for Protecting Privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05), 557-570, 2002.

26. Meyerson A., Williams R., On the Complexity of Optimal k-anonymity, ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, Paris-Fransa, 223-228, 14-16 Haziran, 2004.

27. Li N., Li T., Venkatasubramanian S., t-closeness: Privacy Beyond k-anonymity and l-diversity, IEEE International Conference on Data Engineering, İstanbul-Türkiye,106-115, 15-20 Nisan, 2007.

28. Li N., Li T., Venkatasubramanian S., Closeness: A New Privacy Measure for Data Publishing, IEEE Transactions on Knowledge and Data Engineering, 22(7), 943-956, 2010.

29. Sweeney L., Achieving k-anonymity Privacy Protection Using Generalization and Suppression, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05), 571-588, 2002.

30. LeFevre K., DeWitt D.J., Ramakrishnan R., Incognito: Efficient Full-domain k-anonymity, ACM SIGMOD International Conference on Management of Data, Maryland-ABD, 49-60, 14-16 Haziran, 2005.

31. Kohlmayer F., Prasser F., Eckert C., Kemper A., Kuhn K.A., Flash: Efficient, Stable and Optimal k-anonymity, IEEE International Conference on Privacy, Security, Risk and Trust and International Confernece on Social Computing, Amsterdam-Hollanda, 708-717, 3-5 Eylül, 2012.

32. Sweeney L., Datafly: A System for Providing Anonymity in Medical Data, Database Security XI, IFIP Advances in Information and Communication Technology, Massachusetts, Springer, 356-381, 1998.

33. Wang K., Yu P.S., Chakraborty S., Bottom-up Generalization: A Data Mining Solution to Privacy Protection, IEEE International Conference on Data Mining, Bringhton-İngilitere, 249-256, 1-4 Kasım, 2004.

34. Fung B.C.M, Wang K., Yu P.S., Top-Down Specialization for Information and Privacy Preservation, International Conference on Data Engineering. Tokyo-Japonya, 205-216, 5-8 Nisan, 2005.

35. LeFevre K., DeWitt D.J., Ramakrishnan R., Mondrian Multidimensional k-anonymity, IEEE International Conference on Data Engineering, Atlanta-ABD, 25-25, 3-7 Nisan, 2006.

36. Xiao X., Tao Y., Personalized Privacy Preservation, ACM SIGMOD International Conference on Management of Data, Şikago-ABD, 229-240, 27-29 Haziran, 2006.

37. Samarati P., Protecting Respondents Identities in Microdata Release, IEEE Transactions on Knowledge and Data Engineering, 13(6), 1010-1027, 2001.

38. Skowron A., Rauszer C., The Discernibility Matrices and Functions in Information Systems, Intelligent Decision Support, Cilt 11, Springer, 331-362, 1992.

39. Aggarwal C.C., Outlier Analysis, Springer, Cham, 2017.

40. Han J., Pei J., Kamber M., Data Mining: Concepts and Techniques, Elsevier, 2011.

41. Witten I.H., Frank E., Hall M.A., Pal C.J., Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kaufmann, 2016.

42. Dheeru D., Taniskidou E.K. UCI Machine Learning Repository. http://archive.ics.uci.edu/ml. Yayın tarihi 2017, Erişim tarihi Mart 25, 2018.