Orclever Proceedings of Research and Development
https://doi.org/10.56038/oprd.v2i1.290
OR CLEVER Science & Research Group

Konferans Bildirisi

Veri Merkezli Güvenlik ve Uyumluluk Platformu Geliştirilmesi (Resepsiyon), Uygulama Sonuçlarının Değerlendirilmesi

Mutlu BEKTAŞ[1]*, Tuba Buğdaycı Avşar[2] Kadir Yıldırım[3] Ayşan Usta[4]

[1] Niltek Yazılım Teknolojileri A.Ş., Orcid ID: https://orcid.org/0000-0002-9930-1916
[2] Niltek Yazılım Teknolojileri A.Ş., Orcid ID: https://orcid.org/0000-0001-7490-9653
[3] Niltek Yazılım Teknolojileri A.Ş., Orcid ID: https://orcid.org/0009-0001-5107-1832
[4] Niltek Yazılım Teknolojileri A.Ş., Orcid ID: https://orcid.org/0000-0002-9190-5061
* Corresponded author; e-mail: mutlu.betas@niltekyazilim.com.tr; Tel: +095340373872

(First received October 14, 2023 and in final form December 19, 2023)

3rd International Conference on Design, Research and Development (RDCONF 2023)
December 13 - 15, 2023

Reference: Bektaş, M., Avşar, T., B., Yıldırım, K., Usta, A. Veri Merkezli Güvenlik ve Uyumluluk Platformu Geliştirilmesi (Resepsiyon), Uygulama Sonuçlarının Değerlendirilmesi. Orclever Proceedings of Research and Development,3(1), 78-89.

Özet

Bu çalışma enerji, bankacılık ve bilişim şirketlerinin bilgi sistemlerinde karşılaştığı bazı zorluklara odaklanmaktadır. Özellikle, bu sektörlerdeki sistemlerde şu problemler öne çıkmaktadır: farklı sistemler arasında uyumsuzluklar, aynı verilerin tekrarlanması veya çelişkili olması, farklı sistemlerde aynı dili kullanamama sorunları ve verinin kimin tarafından kontrol edildiğinin belirsiz olması gibi konuları ele alıyor. Bu sorunlara çözüm olarak, yetkilere dayalı dinamik veri gizleme, veri izleme ve kullanıcı davranış analizi gibi tekniklerin bir araya getirilerek kötü niyetli faaliyetlerin tespit edilmesine yönelik bilgiler sunulmaktadır. Yani, çalışma bu sektörlerdeki bilgi sistemlerindeki sorunları ele almaktadır ve bu sorunları çözmek için belirli teknik yaklaşımların birleştirilmesini önermektedir.

Anahtar: Veri güvenliği, veri erişim güvenliği, KVKK, veri maskeleme, Siber Güvenlik

Orclever Proceedings of Research and Development
https://doi.org/10.56038/oprd.v2i1.290
OR CLEVER Science & Research Group

Conference Article

Development of a Data-Centered Security and Compliance Platform (Reception), Evaluation of Application Results

Abstract

This study focuses on some of the challenges faced by energy, banking and information technology companies in information systems. In particular, the following problems come to the fore in systems in these sectors: incompatibilities between different systems, repetition or contradiction of the same data, problems of not being able to use the same language in different systems, and uncertainty about who controls the data. As a solution to these problems, techniques such as authorization-based dynamic data hiding, data monitoring and user behavior analysis are combined to provide information to detect malicious activities. That is, the study considers problems in information systems in these sectors and proposes the combination of certain technical approaches to solve these problems.

Keywords: Data security, data access security, PDPA, data masking, Cyber Security

https://doi.org/10.56038/oprd.v2i1.290

1. Giriş

Çalışma kapsamında hassas verinin keşfini ve güvenlik bakış açısıyla yönetilmesini sağlayacak platformun aşağıdaki genel özelliklere sahip kapsam çerçevesinde geliştirilmiştir.

a) **Veri Keşfi:** KVKK için kişisel veriler, kurumsal iş süreçleri için ticari veriler hassas veriler olarak nitelendirilip, bu verilerin tespiti ve veri güvenliği için yol haritası veri keşfi ile gerçekleştirilmektedir. Yapay zekâ nın alt dalı olan doğal dil işleme ile yapısal ve yapısal olmayan veriler içinde yüksek doğrululuk keşfi, keşif paneli ile envanter ve riskler ortaya çıkartılmaktadır. Keşfedilen veriler Doküman Sınıflandırma, Veritabanı Haritalama, Veri Kümeleme ve Veri Maskeleme işlemleri için kullanılmaktadır [1].

b) **Kullanıcı Davranış Analitiği:** Kullanıcı Davranış Analitiği ile veri güvenliğinin kötü niyetli faaliyetler tarafından tehdit edilmesinin önüne geçmek için kullanıcıların günlük kullanım davranışları işlenerek riskli durumları belirlenmektedir. Veri gizliliğinin, bütünlüğünün ve erişiminin kötü niyetli faaliyetler tarafından ihlali tespit edilebilecek ve veri ihlali iletişimi kurulabilmektedir. Belirlenen riskler kurumların veri güvenliği tasarımı için içeriden veya dışarıdan gelebilecek saldırılar karşısında uygunsuz veri erişimleri platform üzerinden bildirilmektedir.

c) **İzlem ve Denetim:** Veri işleme kayıtları ve kişisel veri ihlallerinin izlenmesi sistem kayıtlarından takip edilebilecek ve veri erişim hakkı, unutulma hakkı, itiraz hakkı gibi KVKK kapsamında korunan hakların ihlali durumları için alarm tanımlanmaktadır.

d) **Dinamik Yetki Kontrolü ve Veri Maskeleme:** Veri güvenliği için son derece önemli bir bileşen olan dinamik yetki kontrolü ve veri maskeleme, veri ihlallerinin şirketleri ve paydaşlarını olumsuz etkilemesinin önüne geçen bir siber güvenlik önlemidir. KVKK gibi kişisel ve özel nitelikli kişisel verilerin korunmasıyla ilgili yasal mevzuatlardan kaçmak yerine, bu mevzuatların yükümlülüklerinin uygulamasına yardım eden sistemlerin en önemli parçasıdır. BT ağını siber tehditler karşısında daha güçlü hale getiriyor. Veri gizliliği tesis edilmesini kolaylaştıran işleyişte veritabanı erişim yöneticisi, çok sayıda veritabanını eş zamanlı olarak kontrol etmek için man-in-the-middle proxy yöntemini kullanacaktır (Microsoft SQL Server, Oracle and Postgresql). Varolan SQL'ler

https://doi.org/10.56038/oprd.v2i1.290

üzerinden yapılan yetkilendirilmemiş erişim taleplerini ve izinlerini engellenmektedir. Böylece veritabanı erişim yöneticisi ve dinamik veri maskelemenin birleşimi veritabanında kapsamlı bir koruma sağlamaktadır [2][3].

e) **Fiziksel/Mantıksal Silme ve Anonimleştirme**: Anonim hale getirme bir veri kümesindeki tüm doğrudan ve dolaylı tanımlayıcıların çıkarılarak veya değiştirilerek ilgili kişinin kimliğinin saptanabilmesinin engellenmesi ya da bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişi ile ilişkilendirilemeyecek şekilde kaybetmesidir. Anonim hale getirilen veri artık kişisel veri niteliklerine sahip olmayacağından, Kanun hükümleri kapsamında değerlendirilemeyecektir. Proje ile yapısal ve yapısal olmayan verilerde anonimleştirme yapılabilecektir. Veri keşfi ile keşfedilen ve izlenen verilerin fiziksel ve mantıksal silme işlemleri de platform üzerinden gerçekleşmektedir [4][5][6].

2. Platform Özellikleri

Veri Merkezli Güvenlik ve Uyumluluk Platformu (Resepsiyon) ile hangi işlemlerin yapıldığına dair şekil-1'de yer almaktadır.

Şekil 1 Platform Kapsamı ve Özellikleri

https://doi.org/10.56038/oprd.v2i1.290

3. Sistem ve Mimari

Platform Mimari ile uluslararası yönergelere ve en iyi uygulamalara uygun olarak tutarlı, eksiksiz ve zamanında işleyen bir yazılım altyapısı oluşturmak ve işletmek için gereken tüm temel hususları planlanmıştır. Mimari gereksinimler doğrultusunda tasarlanan yazılım mimarisinin mimari gereksinimleri karşıladığının ve projenin geliştirilebilir olduğunun eş gözden geçirme süreci ile değerlendirilmesi gerekmektedir. Bu doğrultuda;

- Kalite öznitelikleri, gereksinimleri açıkça tanımlanmış,
- Yazılım mimari dokümantasyonu oluşturulmuş,
- Tasarım kararları gerçekleştirilmiş,
- Mimari riskleri tespit edilmiş,
- Paydaşlar arasında iletişim geliştirilmiş olunması hedeflenmiştir.

3.1 Mimari Prensipler

Mimari tasarım sürecini yönlendirmek için kullanılan bir ilkeler aşağıda listelenmiştir;

- Endişelerin ayrılması (Separation of Concerns): Bileşenler, aralarında karşılıklı bağımlılığı önlemek ve uygulamanın sürdürülmesine yardımcı olmak için bölünmelidir.
- Tek Sorumluluk İlkesi (Single Responsibility Principle): Her bileşenin, kullanıcının sistemi açıkça anlamasını sağlayan belirli bir sorumluluğu olmaktadır. Ayrıca, bileşenin diğer bileşenlerle entegrasyonuna da yardımcı olmaktadır.
    - Basit ve Açık Tut Prensibi (KISS- Keep It Simple Stupid): Gereksiz karmaşıklığı ve özelliklerin aşırı mühendisliğini azaltmak için görevleri yerine getiren en basit çözümler daha karmaşık olanlara tercih edlmektedir.
- Kendinizi Tekrarlamama Prensibi (DRY-Don't Repeat Yourself): Bileşenlerin işlevselliği tekrar edilmemelidir. Bir uygulama içindeki işlevselliğin kopyalanması, değişikliklerin uygulanmasını zorlaştırabilir, netliği azaltabilir ve olası tutarsızlıklara neden olabilir.
- Büyük Tasarımı Önceden Küçültme: Gereksinimleri değiştirme olasılığı varsa, tüm sistem için büyük bir tasarım yapmaktan kaçınılmalıdır.
- Standart protokollerin ve formatların kullanımı: Çeşitli bileşenler arasındaki bilgi alışverişi, yanlış yorumlamaya yer bırakmayacak, iyi tanımlanmış ve standart protokoller üzerinden gerçekleştrilmektedir.

https://doi.org/10.56038/oprd.v2i1.290

3.2. Adlandırma Kuralları

Veritabanı (RDBMS) nesnelerinin adlandırılmasında standart kurallara uyulacaktır. Bu kurallar;

- Her zaman CamelCase veya PascalCase (titlecase) isimlendirme kullanılır.
- Sayı ile başlayan bir isimlendirme yapılmaz.
- Manalı ve uygun isimlendirme yapılır.
- Tüm isimlendirmeler için çok fazla uzun olmuyorsa kısaltma kullanılmaz.
- Bir kısaltma yapacaksanız herkesçe bilinen bir kısaltma seçilir ya da anlaşılabilirdir.
- Tekrarlı ve manasız önek ve ekler kullanılmaz.
- Boolean olan değişkenlere "can", "is" , veya "has" öneki eklenir.
    - Matematiksel bir değişkenlere "Average", "Count", "Sum", "Min", ve "Max" uzantı-ları eklenebilir.
- Camel Case: İsimlerin ilk kelimesinin küçük harfle başlaması sonraki kelimelerin baş harflerinin büyük yazılmasıdır.
- Pascal Case : İsimlerin ilk kelimesin büyük harfle başlaması ve sonra gelen tüm isimlerin baş harflerinin büyük harf olmasıdır.
- Access modifier' ları static yapıcı metotları hariç, her zaman kullanılır. Gerçekten la-zım olan Access modifiersi kullanın varsayılan bile olsa bu özellikle yazılır.

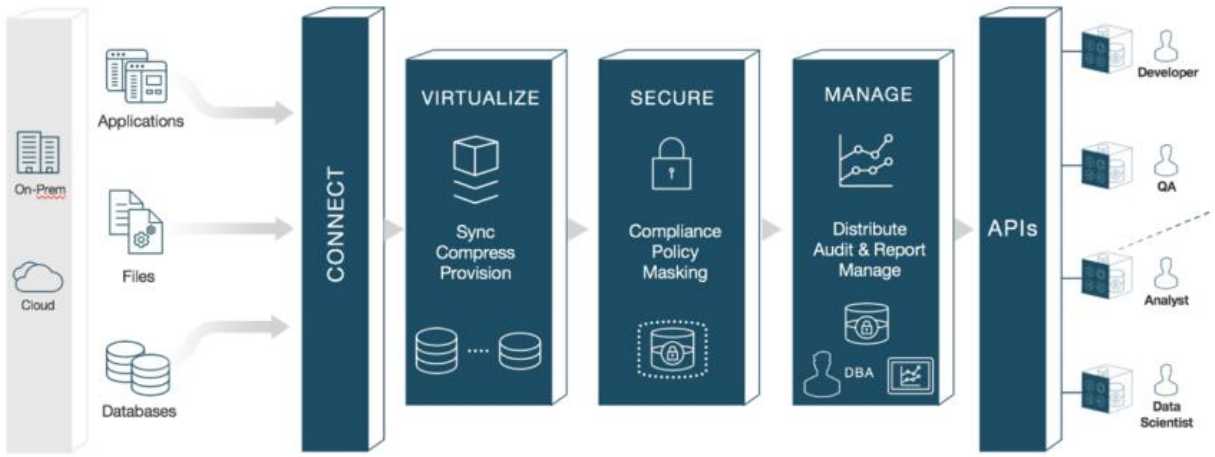
//Kötü
WriteToDB(obj $anObject): void
//Güzel
private WriteToDB(obj $anObject): void

- Numeric değerler (Magic Number) kod içinde kullanılmaz. Constant veya Enum kul-lanılır.
- Recursive methodlar kullanmaktan kaçınılır. Mümkün oldukça loop veya nested lop-lar kullanılır.
- Her zaman çalışan basit şeyler yapın (nesneler) ve zaman buldukça refactoring yapı-lır.
- Kullanıcı User Interface ile İş mantığı ayrılır. Veritabani sorguları, Özel hesaplamaları ve kaynaklara ulaşımı iş mantığı katmanında yapılır.
- Design pattern isimlerini sınıf isimlerinde kullanmaya çalışınız. Ör. UserRepository
- Hem Veritabanı nesnelerinin adlandırılmasında hem de Uygulama bileşenlerinde ön eklerin kullanılması tercih edilir.

3.3. Platform Mimari

Platform mimarisi şekil-2'de gösterilmektedir.

https://doi.org/10.56038/oprd.v2i1.290



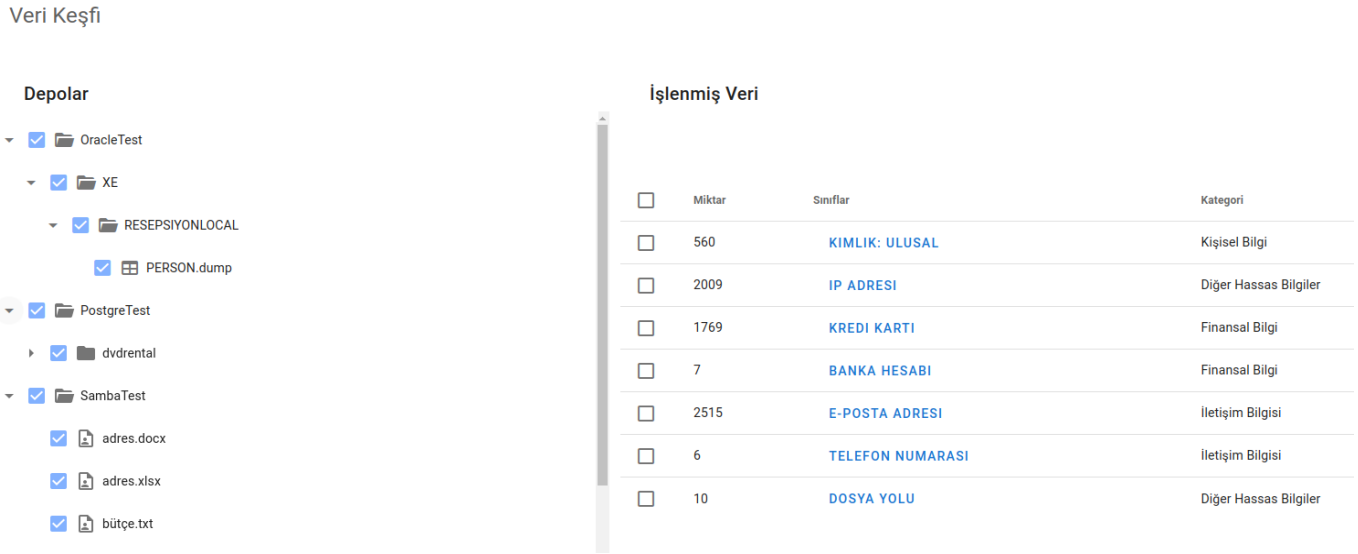
Şekil 2 Platform Mimarisi

4. Platform Uygulama Sonuçları

Geliştirilen resepsiyon platformu (https://resepsiyon.co/) https://test.resepsiyon.co/ adresinde canlıya alınarak veri keşfi, veri kümeleme, doküman sınıflandırma, veritabanı haritalama, veritabanı maskeleme ve doküman maskeleme hizmeti sunmaktadır.

4.1 Veri Keşfi

Şekil 3 de Veritabanı depolarına (PostgreTest ve OracleTest) ve döküman deposuna (SambaTest) ait verilerin keşfi yer almaktadır.

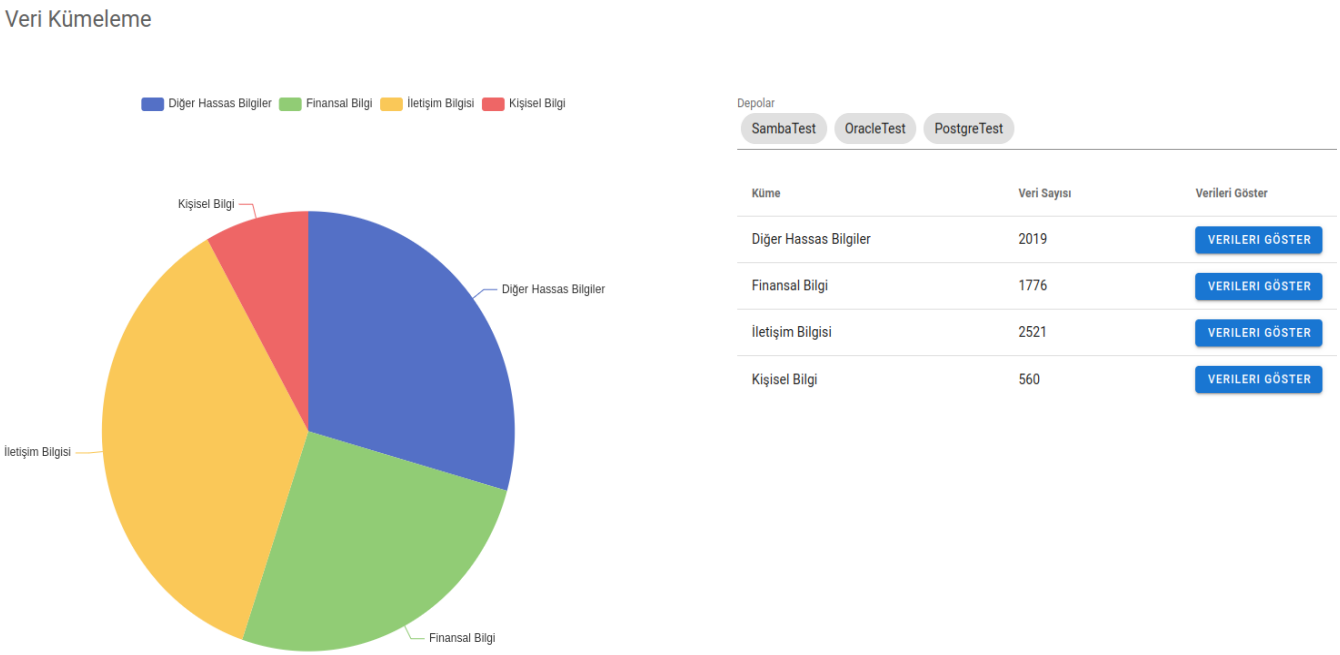


Şekil 3 Veri Keşfi Ekran görüntüsü

https://doi.org/10.56038/oprd.v2i1.290

4.2 Veri Kümeleme

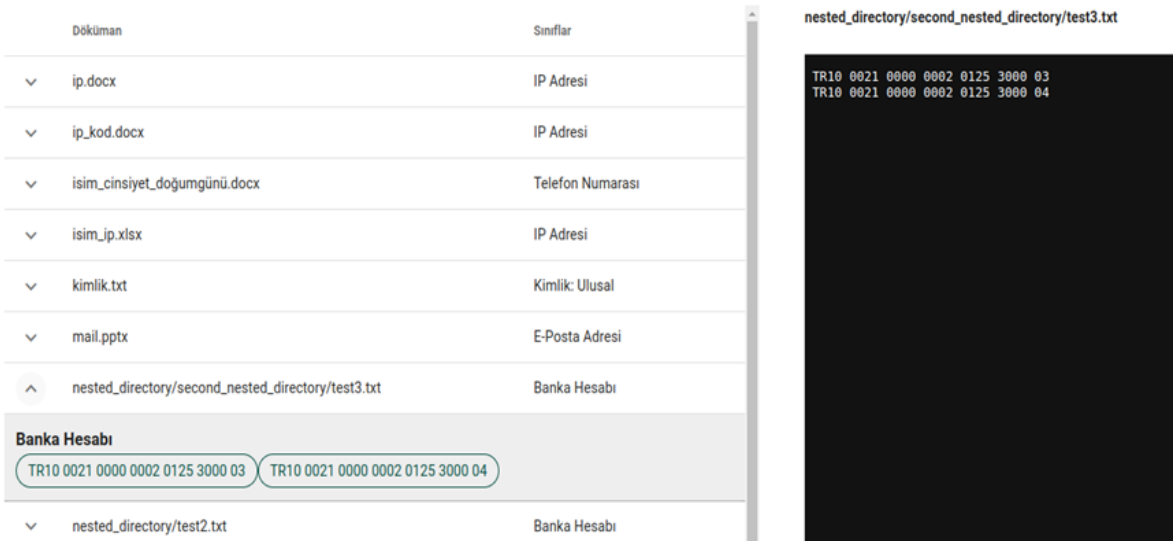
Şekil 4'de, Şekil 3'de keşfedilmiş verilerin sınıflara göre kümelenmesi yer almaktadır.



Şekil 4 Veri Kümeleme Ekran görüntüsü

4.3 Doküman Sınıflandırma

Şekil 5'de dökümanlar içerisindeki verilerin sınıflandırıldığı görülmektedir.

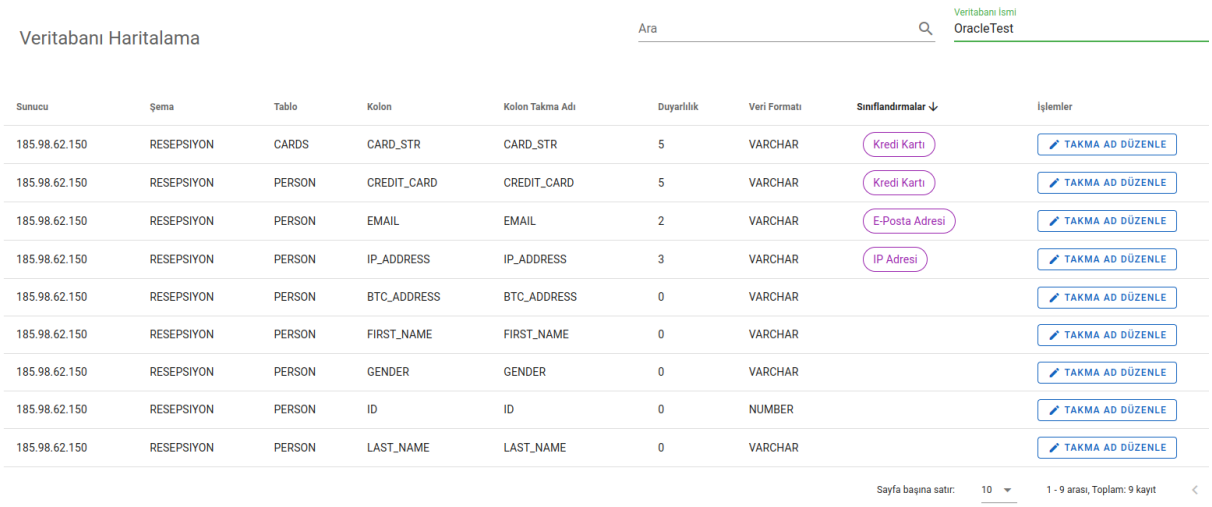


Şekil 5 Doküman Sınıflandırma Ekran görüntüsü

https://doi.org/10.56038/oprd.v2i1.290

4.4 Veritabanı Haritalama

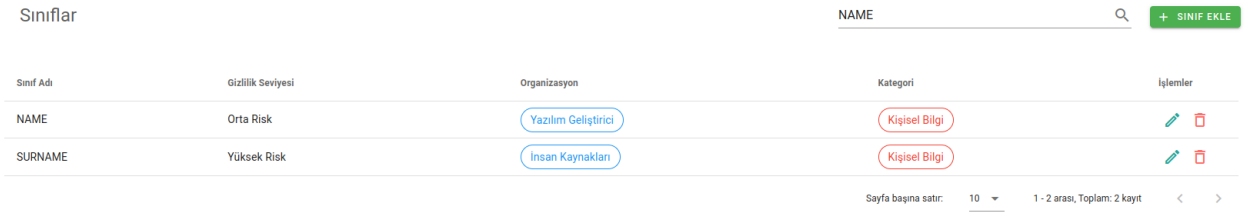
Şekil 6 da Veritabanı kolonlarının, içerdikleri verilere göre sınıflandırıldığı görülmektedir.



Şekil 6 Veritabanı Haritalama Ekran görüntüsü

4.5 Veritabanı Maskeleme

Şekil 7 de Sınıflar ve sınıfların organizasyonlar ile bağlantısı incelendiğinde "NAME" ve "SURNAME" adında iki sınıf ve bu iki sınıfa sırası ile bağlı "Yazılım Geliştirici" ve "İnsan Kaynakları" organizasyonları görülmektedir.



Şekil 7 Sınıflar ve organizasyonlar ile bağlantısı

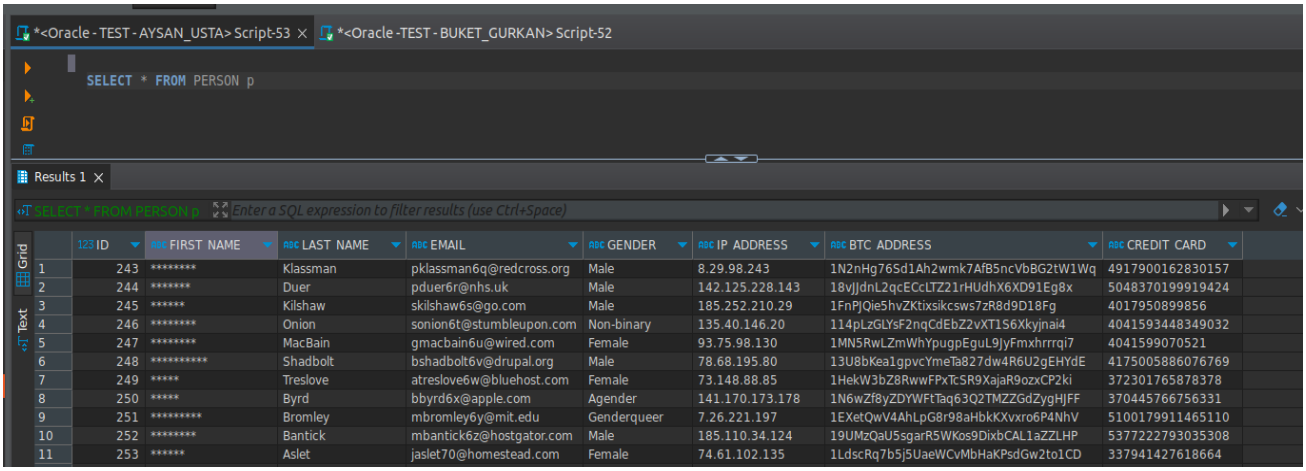
Burada "Yazılım Geliştirici" organizasyonundaki kullanıcılara "NAME" sınıfındaki verilerin, "İnsan Kaynakları" organizasyonundaki kullanıcılara ise "SURNAME" sınıfındaki verilerin maskelenmesi gerektiği ifade edilmektedir.

Şekil 8 de ise kullanıcılar ve kullanıcıların organizasyonlar ile bağlantısı incelendiğinde "Yazılım Geliştirici" organizasyonundaki "Ayşan Usta" kullanıcısı ile ve "İnsan

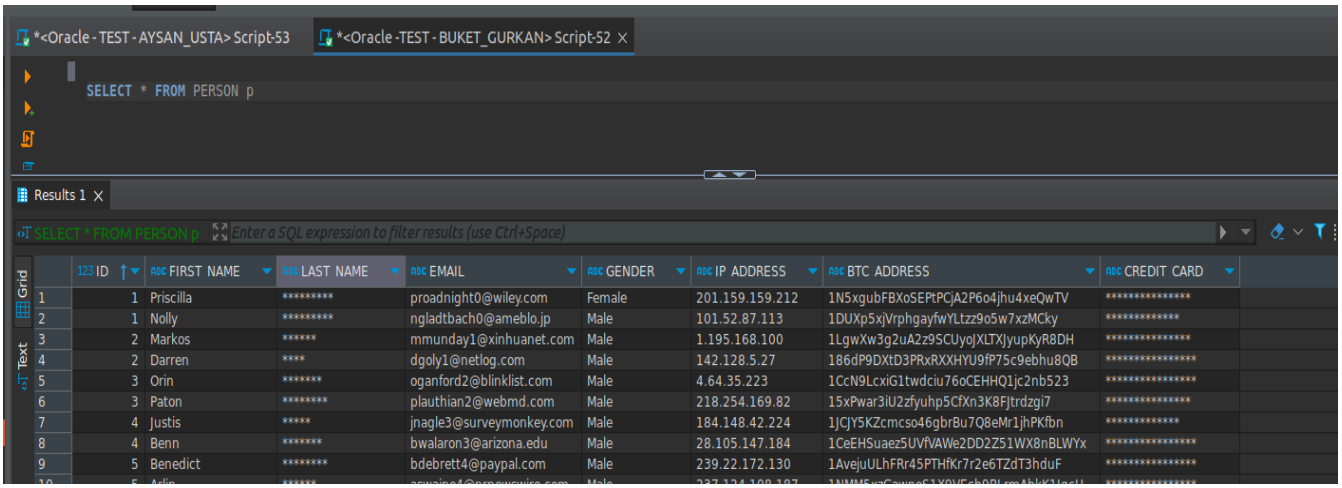
https://doi.org/10.56038/oprd.v2i1.290

Kaynakları" organizasyonundaki "Buket Gürkan" kullanıcısı ile veritabanındaki "PERSON" tablosuna istek atıldığında, Şekil 9 ve Şekil 10 da tablodaki "FIRST_NAME" kolonunun "Ayşan Usta" kullanıcısına, "LAST_NAME" kolonunun ise "Buket Gürkan" kullanıcısına maskelenmiş olduğu görülmektedir.

Şekil 8 Kullanıcılar ve organizasyonlar ile bağlantısı



Şekil 9 "Aysan Usta" kullanıcısı maskeleme

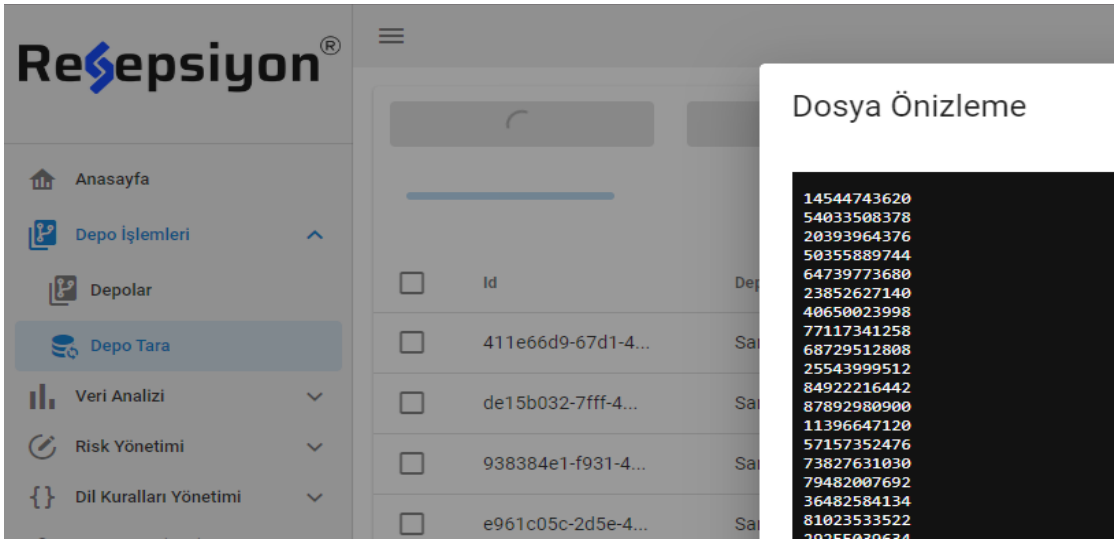


Şekil 10 "Buket Gürkan" kullanıcısı maskeleme

https://doi.org/10.56038/oprd.v2i1.290

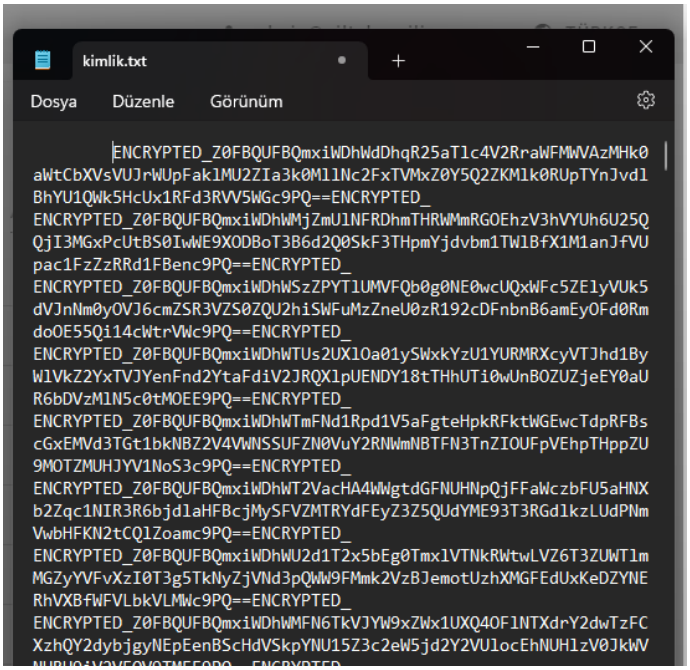
4.6 Döküman Maskeleme

Bu kapsamda gerçek olmayan T.C. kimlik numaraları metin belgesine işlenerek, resepsiyon platformunda işleme alınmıştır. Dosya ön izleme ve veri tarama işlemi öncesine ait ekran görüntüsü şekil-11 de gösterilmektedir.



Şekil 11 Veri Maskeleme Öncesine ait Ekran görüntüsü

Veri maskeleme işlemi sonrasında maskelenen veriye ait ekran görüntüsü şekil-12'de paylaşılmaktadır.



Şekil 12 Makenlenmiş Veri

https://doi.org/10.56038/oprd.v2i1.290

Bulgu sonuçlarından da görüleceği üzere kurumlar arası, departmanlar arası ve tüm sektörlerde verinin oldukça önem arz ettiği günümüzde istenilen verilerin maskelenmesi veri güvenliği açısından kullanışlı ve yaygınlaşma potansiyeli yüksek platform olarak kullanıcılara sunulmaktadır.

5. Sonuçlar

Çalışma ile görüldüğü üzere resepsiyon projesi ile dağıtım şirketlerini veri düzenlemeleriyle KVKK uyumlu hale getirmek ve gelecekteki düzenlemelere hızlı uyum sağlayabilmelerini sağlamak için gerekli Veri Erişim Yönetimi özelliklerine sahip Resepsiyon Veri Güvenliği ve Uyumluluk Platformu geliştirilmiştir.

Bu sayede tek platform üzerinden veritabanlarında bulunan verilerin keşfi, şüpheli davranışların tespiti için kullanıcı davranışı analizi, izleme ve denetim, dinamik yetki kontrolü ve veri maskeleme ile fiziksel/mantıksal silme işlem kabiliyetlerine sahip olunacaktır. Dağıtım şirketlerinin bilgi sistemleri arasındaki entegrasyon zorlukları, mükerrer ve çelişen veriler, bilişim sistemlerinde dil birliği sağlanamaması ve veri sahipliğinin belli olmaması gibi sorunların proje çıktısı platform vasıtasıyla çözüme kavuşacağı öngörülmektedir.

6. Teşekkür

Projenin başarı ile tamamlanmasında desteklerinden dolayı Enerji Piyasası Düzenleme Kurumu (EPDK)'a ve çalışanlarına teşekkür ederiz.

Referanslar

[1] Kişisel Verilerin Korunması Kanunu (Erişim Tarihi: 01.12.2023)
[2] ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı
[3] Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi
[4] Atagün, A. Ö. F. Kişisel Veri Koruma Hukukunda Anonimleştirme
[5] Küzeci, E. (2010). Kişisel verilerin korunması. Ankara: Turhan Kitabevi
[6] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Denetim Rehberi