



Konferans Bildirisi

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

Mutlu BEKTAŞ^{1*}, Tuba Buğdaycı Avşar² Kadir Yıldırım³ Ayşan Usta⁴

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 maskeleyme, Siber Güvenlik



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



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 doğruluk keşfi, keşif paneli ile envanter ve riskler ortaya çıkartılmaktadır. Keşfedilen veriler Doküman Sınıflandırma, Veritabanı Haritalama, Veri Kümeleme ve Veri Maskeleyme 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 Maskeleyme:** Veri güvenliği için son derece önemli bir bileşen olan dinamik yetki kontrolü ve veri maskeleyme, 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

üzerinden yapılan yetkilendirilmemiş erişim taleplerini ve izinlerini engellenmektedir. Böylece veritabanı erişim yöneticisi ve dinamik veri maskeleyen 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 gerçekleştirilmektedir [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



3. Sistem ve Mimari

Platform Mimari ile uluslararası yönergeler 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 Prensipleri (KISS- Keep It Simple Stupid): Gereksiz karmaşıklığı ve özelliklerin aşırı mühendisliğini azaltmak için görevleri yerine getiren en basit çözümler daha karmaşık olanlara tercih edilmektedir.
- Kendinizi Tekrarlamama Prensipleri (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 gerçekleştirilmektedir.



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 yaparsanız herkesçe bilinen bir kısaltma seçilir ya da anlaşılabilir.
- 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 lazım olan Access modifiersi kullanın varsayılan bile olsa bu özellikle yazılır.

//Kötü

WriteToDB(obj \$anObject): void

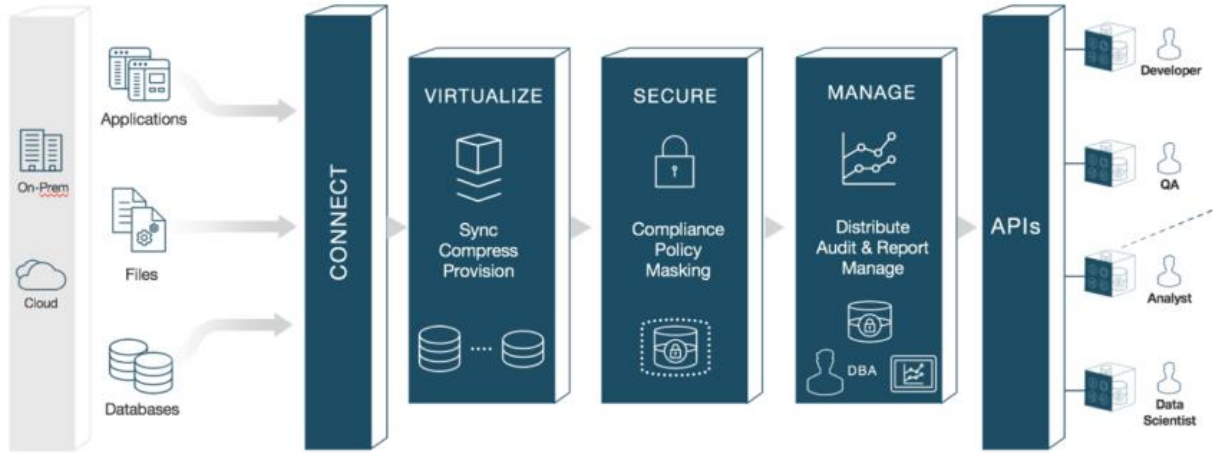
//Güzel

private WriteToDB(obj \$anObject): void

- Numeric değerler (Magic Number) kod içinde kullanılmaz. Constant veya Enum kullanılır.
- Recursive methodlar kullanmaktan kaçınılır. Mümkün oldukça loop veya nested loop-lar kullanılır.
- Her zaman çalışan basit şeyler yapın (nesneler) ve zaman buldukça refactoring yapılır.
- Kullanıcı User Interface ile İş mantığı ayrılır. Veritabanı 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.



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 maskeleye ve doküman maskeleye hizmeti sunmaktadır.

4.1 Veri Keşfi

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

Veri Keşfi

Depolar

OracleTest

XE

RESEPSIYONLOCAL

PERSON.dump

PostgreTest

dvdrental

SambaTest

adres.docx

adres.xlsx

bütçe.txt

İşlenmiş Veri

☐	Miktar	Sınıflar	Kategori
☐	560	KIMLIK: ULUSAL	Kişisel Bilgi
☐	2009	IP ADRESİ	Diğer Hassas Bilgiler
☐	1769	KREDİ KARTI	Finansal Bilgi
☐	7	BANKA HESABI	Finansal Bilgi
☐	2515	E-POSTA ADRESİ	İletişim Bilgisi
☐	6	TELEFON NUMARASI	İletişim Bilgisi
☐	10	DOSYA YOLU	Diğer Hassas Bilgiler

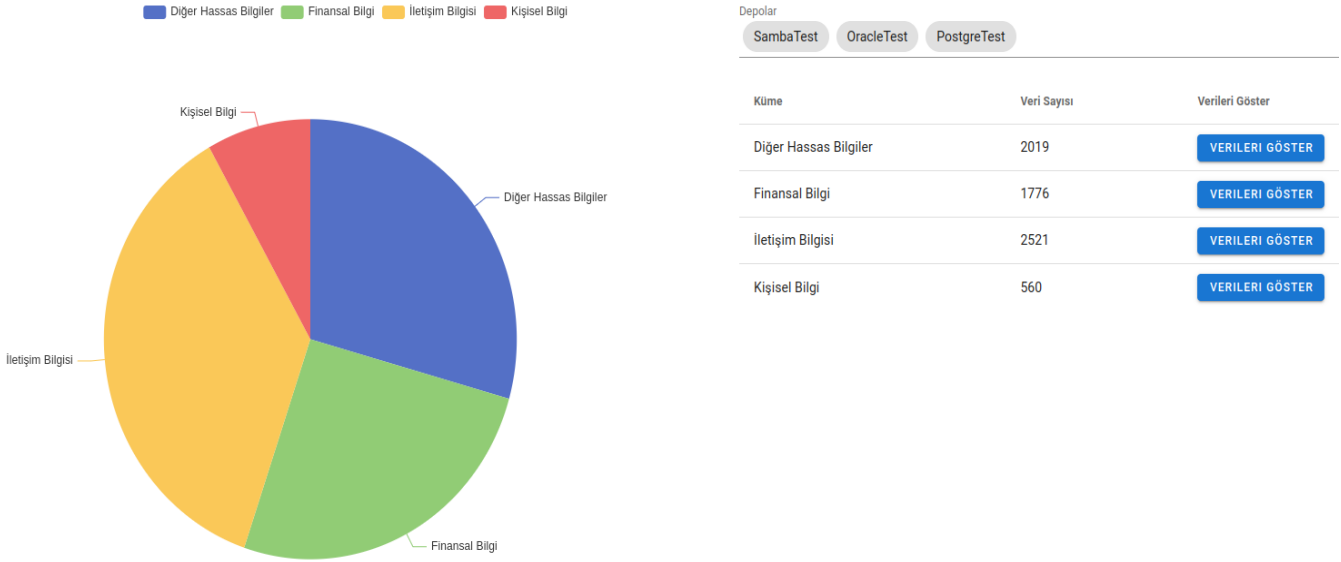
Şekil 3 Veri Keşfi Ekran görüntüsü



4.2 Veri Kümeleme

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

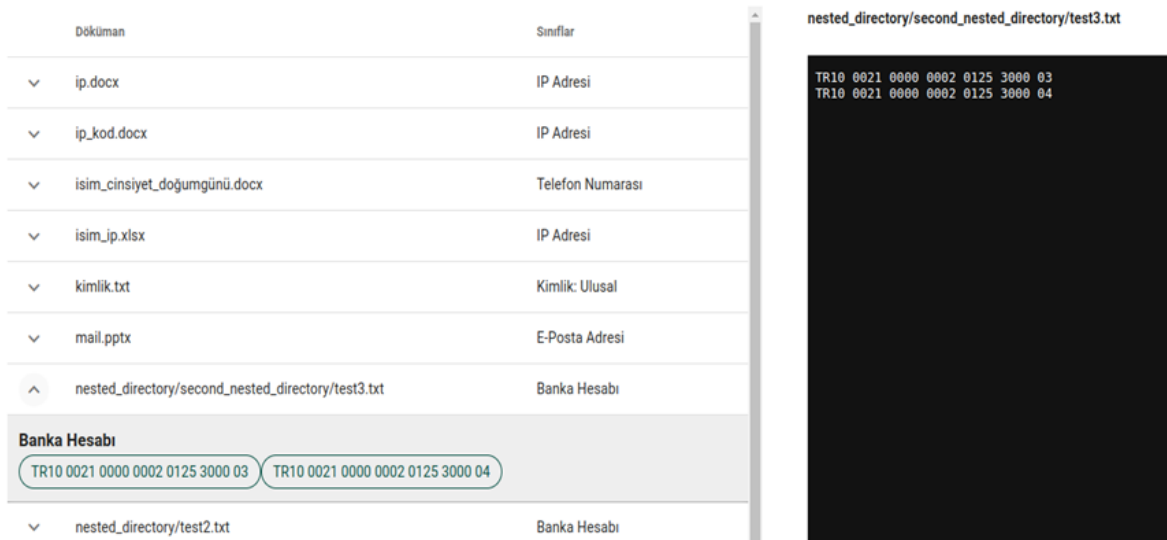
Veri Kümeleme



Şekil 4 Veri Kümeleme Ekran görüntüsü

4.3 Doküman Sınıflandırma

Şekil 5’de dokümanlar içerisindeki verilerin sınıflandırıldığı görülmektedir.



Şekil 5 Doküman Sınıflandırma Ekran görüntüsü



4.4 Veritabanı Haritalama

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

Veritabanı Haritalama

Ara

Veritabanı İsmi
OracleTest

Sunucu	Şema	Tablo	Kolon	Kolon Takma Adı	Duyarlılık	Veri Formatı	Sınıflandırmalar ↓	İşlemler
185.98.62.150	RESEPSİYON	CARDS	CARD_STR	CARD_STR	5	VARCHAR	Kredi Kartı	TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	CREDIT_CARD	CREDIT_CARD	5	VARCHAR	Kredi Kartı	TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	EMAIL	EMAIL	2	VARCHAR	E-Posta Adresi	TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	IP_ADDRESS	IP_ADDRESS	3	VARCHAR	IP Adresi	TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	BTC_ADDRESS	BTC_ADDRESS	0	VARCHAR		TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	FIRST_NAME	FIRST_NAME	0	VARCHAR		TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	GENDER	GENDER	0	VARCHAR		TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	ID	ID	0	NUMBER		TAKMA AD DÜZENLE
185.98.62.150	RESEPSİYON	PERSON	LAST_NAME	LAST_NAME	0	VARCHAR		TAKMA AD DÜZENLE

Sayfa başına satır:10

1 - 9 arası, Toplam: 9 kayıt

Şekil 6 Veritabanı Haritalama Ekran görüntüsü

4.5 Veritabanı Maskeleye

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.

Sınıflar				NAME	+ SINIF EKLE
Sınıf Adı	Gizlilik Seviyesi	Organizasyon	Kategori	İşlemler	
NAME	Orta Risk	Yazılım Geliştirici	Kişisel Bilgi		
SURNAME	Yüksek Risk	İnsan Kaynakları	Kişisel Bilgi		

Sayfa başına satır: 10 1 - 2 arası, Toplam: 2 kayıt

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



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

Kullanıcılar

Ara

+

LDAP KULLANICI EKLE

+

YENİ KULLANICI EKLE

Ad	Soyad	E-posta	Organizasyon	Domain	Oluşturulma	İşlemler
Aysan	Usta	aysan.usta@niltekyazilim.com.tr	Yazılım Geliştirici	niltekyazilim.com	24/11/2023 09:33	 
Buket	Gürkan	buket.gurkan@niltekyazilim.com.tr	İnsan Kaynakları	niltekyazilim.com	23/11/2023 12:00	 

Şekil 8 Kullanıcılar ve organizasyonlar ile bağlantısı

*Oracle - TEST - AYSAN_USTA> Script-53

*Oracle - TEST - BUKET_GURKAN> Script-52

SELECT * FROM PERSON p

Results 1

Enter a SQL expression to filter results (use Ctrl+Space)

	ID	FIRST NAME	LAST NAME	EMAIL	GENDER	IP ADDRESS	BTC ADDRESS	CREDIT CARD
1	243	*****	Klassman	pklassman6q@redcross.org	Male	8.29.98.243	1N2nHg765d1Ah2wmk7AF85ncVbBG2tW1Wq	4917900162830157
2	244	*****	Duer	pduer6r@nhs.uk	Male	142.125.228.143	18VJdnL2qcECcLTZ21rHudhX6XD91Eg8x	5048370199919424
3	245	*****	Kilshaw	skilshaw6s@go.com	Male	185.252.210.29	1FnPJQie5hvZKtksiccsws7zR8d9D18Fg	4017950899856
4	246	*****	Onion	sonion6t@stumbleupon.com	Non-binary	135.40.146.20	114pLzGLYsF2ngCdEbZ2vXT1S6Xkyjnal4	4041593448349032
5	247	*****	MacBain	gmabbain6u@wired.com	Female	93.75.98.130	1MN5RwLZmWhYpugEguL9jYFmxhrrrq7	4041599070521
6	248	*****	Shadbolt	bshadbolt6v@drupal.org	Male	78.68.195.80	13U8bKea1gpvcYmeTa827dw4R6U2gEHYdE	4175005886076769
7	249	*****	Treslove	atreslove6w@bluehost.com	Female	73.148.88.85	1HekW3bZ8RwwFPxTSR9XajaR9ozxCP2ki	372301765878378
8	250	*****	Byrd	bbyrd6x@apple.com	Agender	141.170.173.178	1N6wZf8yZDYWFTaq63Q2TMZZGdZygHJFF	370445766756331
9	251	*****	Bromley	mbromley6y@mit.edu	Genderqueer	7.26.221.197	1EXetQwV4AhLpG8r98aHbkKXvro6P4NhV	5100179911465110
10	252	*****	Bantick	mbantick6z@hostgator.com	Male	185.110.34.124	19UMzQaU5sgarR5Wkos9DixbCAL1aZZLHP	5377222793035308
11	253	*****	Aslet	jaslet70@homestead.com	Female	74.61.102.135	1LdscRq7b5j5UaeWCVmBHaKpPdGw2to1CD	337941427618664

Şekil 9 “Aysan Usta” kullanıcısı maskeleyme

*Oracle - TEST - AYSAN_USTA> Script-53

*Oracle - TEST - BUKET_GURKAN> Script-52 X

SELECT * FROM PERSON p

Results 1 X

Enter a SQL expression to filter results (use Ctrl+Space)

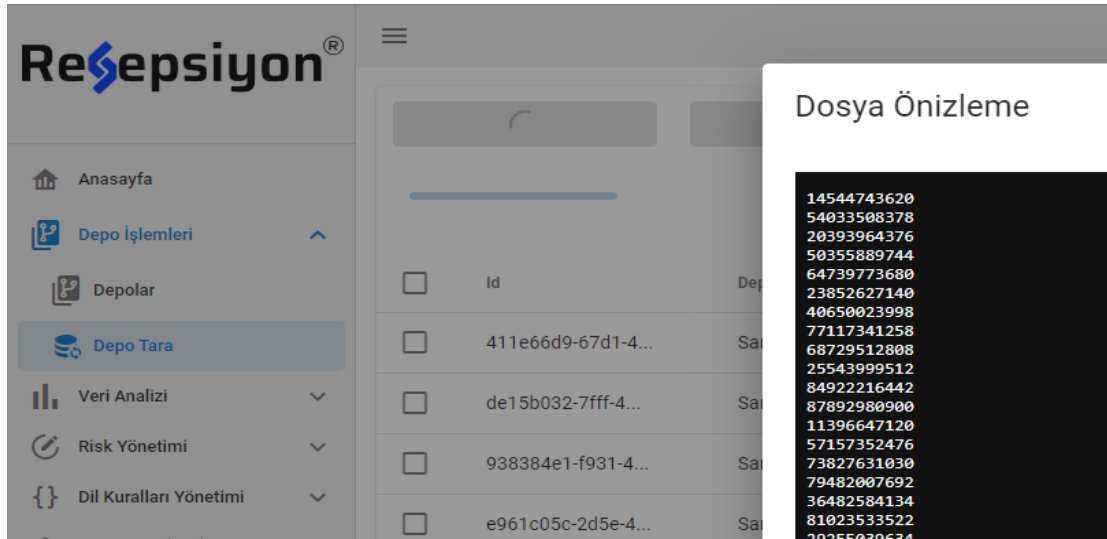
	123 ID ↑	ASC FIRST NAME	ASC LAST NAME	ASC EMAIL	ASC GENDER	ASC IP ADDRESS	ASC BTC ADDRESS	ASC CREDIT CARD
1	1	Priscilla	*****	proadnight0@wiley.com	Female	201.159.159.212	1N5xgubFBXo5EPIPCjA2P6o4jhu4xeQwTV	*****
2	1	Nolly	*****	ngladtbach0@ameblo.jp	Male	101.52.87.113	1DUXp5xjVrphgayfwYLTz9o5w7xzMcKY	*****
3	2	Markos	*****	mmunday1@xinhuanet.com	Male	1.195.168.100	1LgwXw3g2uA2z9SCUyqjXLTjyupKyR8DH	*****
4	2	Darren	****	dgo1y1@netlog.com	Male	142.128.5.27	186dP9DXtD3PRxRXXHYU9fP75c9ebhu8QB	*****
5	3	Orin	*****	oganford2@blinklist.com	Male	4.64.35.223	1CcN9LxiG1twdciu76oCEHHQ1jc2nb523	*****
6	3	Paton	*****	plauthian2@webmd.com	Male	218.254.169.82	15xPwar3lU2zfuyhp5Cfkn3K8Fjtrdzg7	*****
7	4	Justis	****	jnagle3@surveymonkey.com	Male	184.148.42.224	1CjY5KZcmcs046gbrBu7Q8eMr1jhPKfbn	*****
8	4	Benn	*****	bwalaron3@arizona.edu	Male	28.105.147.184	1CeHSuaez5UVfVAWe2DD2Z51WX8nBLWyx	*****
9	5	Benedict	*****	bdebrett4@paypal.com	Male	239.22.172.130	1AvejuULHFr45PTHfk7r2e6TZd2T3hduF	*****
10	5	Arlo	*****	aroulet6@comcast.net	Male	232.134.109.187	1UMMfWwCaup651X0VfGsh0PmzAbhG1uyH1	*****

Şekil 10 “Buket Gürkan” kullanıcısı maskeleyme



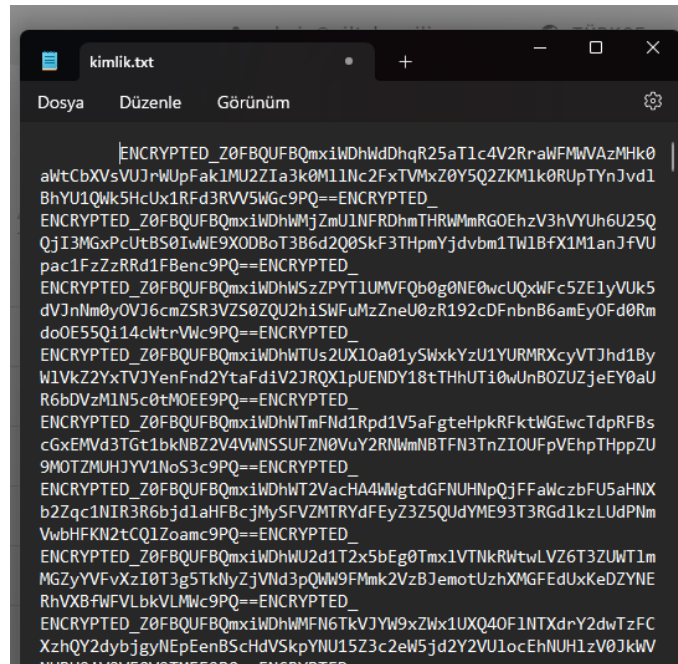
4.6 Döküman Maskeleme

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



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 maskeleyme 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