ÖZET

BİR KRİTİK VERİ TARAMA SİSTEMİ

Bu buluş, kişisel verilerin korunması kanunu (KVKK) kapsamında kritik veri olarak belirlenen alanların veri tabanı meta datalarında taranmasını, kritik veri alanlarının birincil anahtar (primary key) olarak tanımlanmamasının kontrolünü sağlayan ve hatalı kullanım durumlarından bilgilendirilme yapılmasını sağlayan bir sistem (1) ile ilgilidir.

İSTEMLER

1. Kritik veri olarak belirlenen alanların veri tabanı meta datalarında taranmasını, kritik veri alanlarının birincil anahtar (primary key) olarak tanımlanmamasının kontrolünü sağlayan buluş konusu sistem (1);
-en azından kullanıcıların kullanıcı girişi yapmalarını ve kritik veri araması yapmak istediği veri tabanlarını seçmelerine olanak sağlamak üzere yapılandırılan en az bir uygulama (2) ve
-herhangi bir iletişim protokolünü kullanarak uygulama (2) ile veri alışverişi gerçekleştirmek, uygulama (2) üzerinden seçilen veri tabanının verisini çekmek, sonrasında sinir ağı sınıflandırması algoritması kullanılarak veri tabanının meta datasında kritik veri içeren kolon isimleri taramak, tarama sonucu bulunan verileri kritik veri olarak kayıt altına almak ve yeni tarama işlemlerinde kayıt altına alınan kritik verileri karşılaştırma amaçlı kullanmak ve karşılaştırma sonucunda kritik veriye ulaştığında alarm üretmek üzere yapılandırılan en az bir sunucu (3) **ile karakterize edilen** bir sistem (1).

2. Sunucu (3) ile iletişimde olup veri alışverişi gerçekleştirmek üzere yapılandırılan uygulama (2) **ile karakterize edilen** İstem 1'deki gibi bir sistem (1).

3. Sunucu (3) tarafından kullanıcı girişi doğrulamasına tabi tutulacak kullanıcıya ait kullanıcı bilgilerini almak ve sunucu (3) ile paylaşmak üzere yapılandırılan uygulama (2) **ile karakterize edilen** İstem 1 veya 2'deki gibi bir sistem (1).

4. Aldığı kullanıcı bilgileri ile LDAP (Lightweight Directory Access Protocol) üzerinden kimlik doğrulama ve yetki doğrulama işlemlerini yapmak üzere yapılandırılan sunucu (3) **ile karakterize edilen** yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

5. Herhangi bir uzak iletişim protokolünü kullanarak uygulama (2) ile veri alışverişi gerçekleştirmek üzere yapılandırılan sunucu (3) **ile karakterize edilen** yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

6. Uygulama (2) ile kurulan iletişim üzerinden kullanıcı bilgilerini almak, yetki ve kimlik doğrulama işlemine tabi tutmak ve yetkisi olan veri tabanları listelemek üzere yapılandırılan sunucu (3) **ile karakterize edilen** yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

7. Kullanıcının kritik veri taraması yapmak istediği veri tabanı bilgisini almak, söz konusu veri tabanın Meta Datasını çekmek ve üzerinde sinir ağı sınıflandırması algoritması kullanılarak KVKK kapsamında kritik veri içeren kolon isimlerini taramak üzere yapılandırılan sunucu (3) **ile karakterize edilen** yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

8. Algoritma kapsamında mevcutta tespit edilmiş tüm kritik veri kullanımlarını bir kural seti olarak tutmak ve yeni taramada karşılaştırma amaçlı kullanmak üzere yapılandırılan sunucu (3) **ile karakterize edilen** yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

9. Karşılaştırma kapsamında sinir ağı sınıflandırma algoritmasındaki sınıflandırma, tahmin, veri ilişkilendirme özellikleri kullanılarak tespit sağlamak üzere yapılandırılan sunucu (3) **ile karakterize edilen** yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

10. Tespit edilen kritik veri kullanımlarını taranan veri tabanı bilgisi ile birlikte yetkili kişilere bildirmek üzere yapılandırılan sunucu (3) **ile karakterize edilen** yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

TARİFNAME

BİR KRİTİK VERİ TARAMA SİSTEMİ

Teknik Alan

Bu buluş, kişisel verilerin korunması kanunu (KVKK) kapsamında kritik veri olarak belirlenen alanların veri tabanı meta datalarında taranmasını, kritik veri alanlarının birincil anahtar (primary key) olarak tanımlanmamasının kontrolünü sağlayan ve hatalı kullanım durumlarından bilgilendirilme yapılmasını sağlayan bir sistem ile ilgilidir.

Önceki Teknik

KVKK yani kişisel verilerin korunması kanunu kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir. Söz konusu kanunun amaçlarından biri kişisel verilerin işlenmesinin disiplin altına alınmasıdır. Bu nedenle günümüzde kritik veri olarak da kişisel verilerin kullanım alanlarının kontrol edilerek hatalı kullanımların bildirilmesini sağlayarak firmaları, kurumları sıkıntıya sokacak durumlardan kurtaracak çözümlere ihtiyaç duyulmaktadır.

Tekniğin bilinen durumunda yer alan US8407194 sayılı Birleşik Devletler patent dokümanında veri sınıflandırma ve gizlilik havuzu oluşturma sisteminden bahsedilmektedir. Söz konusu Birleşik Devletler patent dokümanına konu olan buluş içerisinde bir kuruluşun özel veya hassas veya kişisel olarak tanımlanabilen bilgilerinin envanterini çıkarmak için güvenli ve doğru bir veri tabanı oluşturmaya yönelik bir veri sınıflandırması ve ilgili kuruluşun kurumsal veri tabanıyla bağlantı kuran en az bir Meta Veri Kaydı bulundurmaktadır. Meta Veri Kaydı, ilgili kurumsal veri tabanında depolanan dosyaları tarar, analiz eder ve sınıflandırır ve

ardından bu dosyalarla ilişkili meta verileri dizinlenebilir bir biçimde barındırır. Bir düzenlemede, meta veriler, meta verilerin doğrulandığı, izlendiği ve risk açısından değerlendirildiği bir hizmet sağlayıcı/sistem yöneticisi Toplu Meta Veri Havuzuna taşınır. Bir ihlal meydana geldiğinde, uygun kişilere, şirketlere, düzenleyici kurumlara ve devlet kurumlarına bildirimler otomatik olarak oluşturulur.

Buluşun Kısa Açıklaması

Bu buluşun amacı, KVKK kapsamında kritik veri olarak belirlenen alanların veri tabanı meta datalarında taranmasını, ilgili kritik veri alanlarının birincil anahtar (primary key) olarak tanımlanmamasının kontrolünün gerçekleştirilmesini ve hatalı kullanım durumunda oluşturulan spesifik alarm mekanizmalarıyla alarmlar üretilip ilgili kişileri bilgilendirilmesini sağlayan bir sistem gerçekleştirmektir.

Buluşun Ayrıntılı Açıklaması

Bu buluşun amacına ulaşmak için gerçekleştirilen "Bir Kritik Veri Tarama Sistemi" ekli şekilde gösterilmiş olup, bu şekil;

Şekil 1 Buluş konusu sistemin şematik görünüşüdür.

Şekilde yer alan parçalar tek tek numaralandırılmış olup, bu numaraların karşılıkları aşağıda verilmiştir:

1. Sistem
2. Uygulama
3. Sunucu

Kritik veri olarak belirlenen alanların veri tabanı meta datalarında taranmasını, kritik veri alanlarının birincil anahtar (primary key) olarak tanımlanmamasının kontrolünü sağlayan buluş konusu sistem (1);

-en azından kullanıcıların kullanıcı girişi yapmalarını ve kritik veri araması yapmak istediği veri tabanlarını seçmelerine olanak sağlamak üzere yapılandırılan en az bir uygulama (2) ve

-herhangi bir iletişim protokolünü kullanarak uygulama (2) ile veri alışverişi gerçekleştirmek, uygulama (2) üzerinden seçilen veri tabanının verisini çekmek, sonrasında sinir ağı sınıflandırması algoritması kullanılarak veri tabanının meta datasında kritik veri içeren kolon isimleri taramak, tarama sonucu bulunan verileri kritik veri olarak kayıt altına almak ve yeni tarama işlemlerinde kayıt altına alınan kritik verileri karşılaştırma amaçlı kullanmak ve karşılaştırma sonucunda kritik veriye ulaştığında alarm üretmek üzere yapılandırılan en az bir sunucu (3) içermektedir.

Buluş konusu sistemde (1) yer alan uygulama (2) sunucu (3) ile iletişimde olup veri alışverişi gerçekleştirmek üzere yapılandırılmaktadır. Uygulama (2) sunucu (3) tarafından kullanıcı girişi doğrulamasına tabi tutulacak kullanıcıya ait kullanıcı bilgilerini almak ve sunucu (3) ile paylaşmak üzere yapılandırılmaktadır. Sunucu (3) aldığı kullanıcı bilgileri ile LDAP (Lightweight Directory Access Protocol) üzerinden kimlik doğrulama ve yetki doğrulama işlemlerini yapmak üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) yer alan sunucu (3), herhangi bir uzak iletişim protokolünü kullanarak uygulama (2) ile veri alışverişi gerçekleştirmek üzere yapılandırılmaktadır. Sunucu (3) uygulama (2) ile kurulan iletişim üzerinden kullanıcı bilgilerini almak, yetki ve kimlik doğrulama işlemine tabi tutmak ve yetkisi olan veri tabanları listelemek üzere yapılandırılmaktadır. Sunucu (3) kullanıcının kritik veri taraması yapmak istediği veri tabanı bilgisini almak, söz konusu veri tabanın Meta Datasını çekmek ve üzerinde sinir ağı sınıflandırması algoritması kullanılarak KVKK kapsamında kritik veri içeren kolon isimlerini taramak üzere yapılandırılmaktadır. Sunucu (3) algoritma kapsamında mevcutta tespit edilmiş tüm kritik veri kullanımlarını bir kural seti olarak tutmak ve yeni taramada karşılaştırma amaçlı kullanmak üzere yapılandırılmaktadır. Sunucu (3)

karşılaştırma kapsamında sinir ağı sınıflandırma algoritmasındaki sınıflandırma, tahmin, veri ilişkilendirme özellikleri kullanılarak tespit sağlamak üzere yapılandırılmaktadır. Sunucu (3) tespit edilen kritik veri kullanımlarını taranan veri tabanı bilgisi ile birlikte yetkili kişilere bildirmek üzere yapılandırılmaktadır.

Buluş konusu sistem (1) sayesinde KVKK kapsamında uyguna olmayan kriterler meta data verisi üzerinde taranarak bulunması durumunda alarm verilmekte, birincil anahtar (primary key) olarak tanımlanmamasının önüne geçilmesi için ilgili birimler bilgilendirilmektedir. Örnek olarak meta datada daha önce taranan ve kritik veri olduğu tespit edilen kimlik verisi alanı yeni tarama başlatılan metadata benzerinin bulunması için dayanak olarak kullanılmaktadır. Bu sayede bir sonraki arama bulunan benzeri kolanlar için alarm üretilmekte ve kullanıcılar bilgilendirilmektedir.

Buluş konusu sistem (1) kullanıcıya veri gizliliği ilkeleri içeren bilgilendirme ve onay sunmakta olup, Kişisel Verilerin Korunması Kanunu (KVKK) dahilinde faaliyet göstermektedir.

Bu temel kavramlar etrafında, buluş konusu “Bir Kritik Veri Tarama Sistemi (1)” ile ilgili çok çeşitli uygulamaların geliştirilmesi mümkün olup, buluş burada açıklanan örneklerle sınırlandırılamaz, esas olarak istemlerde belirtildiği gibidir.

Şekil 1

