SETSCI conference proceedings
SETSCI Conference Proceedings
14 , 49-52, 2022

6th International Symposium on Innovative Approaches in Smart Technologies
December 8-10, 2022, Turkey

ISAS WINTER-2022

https://doi.org/10.36287/setsci.5.2.011

Kurumsal Kaynak Planlaması Yazılımlarında Bilgi Güvenliğini Esas Alan Özel Yetkilendirme Yaklaşımı

Ozan Gelincik[1*] and Nisa Şahinyılmaz[2]

[1] MBIS Ar-Ge Merkezi, Maltepe, İstanbul, Türkiye
[2] MBIS Ar-Ge Merkezi, Maltepe, İstanbul, Türkiye
*Sorumlu yazar: ozan.gelincik@mbis.com.tr
+Konuşmacı: nisa.sahinyilmaz@mbis.com.tr

Özet – Dünyada ve ülkemizde yaygın olarak kullanılan ERP (kurumsal kaynak planlaması) yazılımı olan SAP, kullanıcısı olan şirketlerin sistemlerinde kurum özelinde veri tutmasına olanak sağlamaktadır. Kurum verilerinin gizliliği, kurumların ticari sırlarıdır. Ticari sır niteliği taşıyan kritik bilgiler (ürün formülleri, satın alma fiyat bilgileri, stok bilgileri vb.) veri yönetimine ilişkin regülasyonlar ve tutulan bu kritik bilgilerin içerisinde kişisel verilerin korunmasının önem kazanması gibi değişimler, verinin niteliğini değiştirmiş ve hassasiyetini arttırmıştır. Bu kapsamda alan bazlı yetkilendirme yaklaşımları doğmuş ve verinin granüler bazda yönetimi tüm kurumlar için büyük bir ihtiyaç haline gelmiştir. İlgili verilere erişim yetkilendirilmeli ve talep edilmesi halinde bu erişimler yetkili kişi ve kurullara iletilmelidirler. SAP gibi yaygın olarak kullanılan ERP sistemlerinde yetkilendirme fonksiyonel ve organizasyonel bazlı yapılmaktadır. Ticari sır niteliği taşıyan kritik bilgileri ya da kişisel verileri içeren alanlar, diğer verilerin tutulduğu alanlarla aynı fonksiyonun içerisinde yer aldığından, erişimi fonksiyonel ve organizasyonel bazda yetkilendirmek yeterli olamamaktadır. Alan bazlı yetkilendirme yöntemi aracılığıyla ilgili alanlara erişimler denetim altına alınabilecektir.

Anahtar Kelimeler – ERP, Kurumsal kaynak planlaması, SAP, Alan bazlı yetkilendirme, KVKK, Bilgi ve Sistem güvenliği, Veri yapıları ve Veri yönetimi

I. GİRİŞ

Hızla gelişen bilişim teknolojileri, bilginin saklanması, paylaşılması ve transferinde sağladığı olanaklar ile işletmelere çok büyük fayda ve avantajlar sağladığı için çoğu işletme, faaliyetlerini gerçekleştirmek amacıyla bu teknolojilere bağımlı hale gelmiştir [1]. Bilişim teknolojilerinin günlük hayatta ve iş hayatında yaygınlaşması, sağladığı bu bilgiler arasında gittikçe artan bir ölçüde kişisel verilerin de yer alması, söz konusu verilerin korunması ihtiyacını gündeme getirmiştir [2]. Gerek yerel gerekse uluslararası düzenlemeler ile veri güvenliği denetimlerinin başlaması, daha detaylı bir yetkilendirme yapısına ihtiyacı ortaya çıkarmıştır. ERP sistemleri ki özellikle SAP sistemi, dünyanın birçok ülkesinde ve şirketinde yaygın olarak uygulanmaktadır [3]. Şirketlerin ihtiyaç duyduğu ERP niteliklerinin artması, bu nitelikleri karşılamak için yapılması gereken geliştirmelerin sayısı ile kapsamını da arttırmakta ve iş birimleri tarafından kontrolü ve takibini zorlaştırmaktadır. Bunun yanı sıra standartta çok mümkün olmayan, alan bazlı geliştirmelerin SAP gibi sistemlerde standart roller ile ilişkilendirilmesi ve dış ya da iç denetim ekiplerince denetlenmesi durumu ortaya çıkmaktadır. 'Rol bazlı erişim kontrolü' metodolojisi kullanılarak yaratılan ve 5 katmanlı bir yapıya sahip olan (1- Kullanıcı, 2- Profil, 3- Yetki, 4-Yetki Nesnesi, 5-Nesne Sınıfı) SAP yetkilendirme mimarisi, kullanıcı yetkilendirmelerinin Fonksiyonel ve Organizasyonel bazda başarıyla yönetilmesini sağlamaktadır. [4] SAP/Yetkilendirme düzeyi görseli şekilde 1'de görülmektedir.

Şekil 1. SAP/Yetkilendirme düzeyi

SAP sistemi, standart kapsamında alan bazlı yetkilendirme gibi bir uygulama sunmamaktadır. Ancak user-exit, BADI benzeri geliştirme altyapısı ya da 'ekran varyantı' gibi ek özelliklerle ve ek lisanslarla bu ihtiyacı karşılayan çözümlerin geliştirilmesine olanak tanımaktadır.

SAP kullanan firmalar, 'AURA' ismini verdiğimiz bu çözümümüz sayesinde verinin granüler bazda yönetimi yetkinliklerine sahip olacaklar ve ek bir yazılıma gerek duymadan tek bir sistem içerisinde sahip olabileceklerdir.

II. YÖNTEM

'AURA' içeriğinde barındırdığı ön tanımlı veya gereksinimlere göre tanımlanabilecek koşul ve kurallar kapsamında, SAP' deki standart veya standart dışı ekranlar için alan bazında dinamik yetkilendirme ve alan gizleme işlevlerini yerine getirebilen bir add-on olarak SAP içerisinde ABAP kodlama dilinde geliştirilmiş bir çözümdür.

Çözümün amacı ek geliştirme gereksinimlerini ortadan kaldırıp sadece kural oluşturarak bilgi güvenliği kapsamında alan erişimlerinin özel yetkiye bağlanmasını sağlamaktır.

Alan bazlı yetkilendirme ihtiyacını net bir biçimde ifade edebilmek adına, konuyla ilgili bazı örnekler şu şekilde sıralanabilir;

- Satış siparişlerinde malzeme tanımının görülebilmesi ancak değiştirilememesi
- Stok takip raporlarından miktar bilgisi görülebilir iken stok değerine ilişkin fiyat bilgilerinin gizlenmesi
- Fatura girişlerinde kur bilgisinin görülebilmesi ancak değiştirilememesi
- Personel raporlarında maaş bilgisinin gösterilmemesi
- Satın alma siparişlerinde vade bilgisinin değiştirilememesi
- Ürün reçetelerinde bileşen isimlerinin gizlenmesi

A. *TEMEL FONKSİYONLAR*

Çalışma kapsamında geliştirilen çözümün, alan özelinde uygulayabildiği temel fonksiyonlar aşağıdaki gibidir:

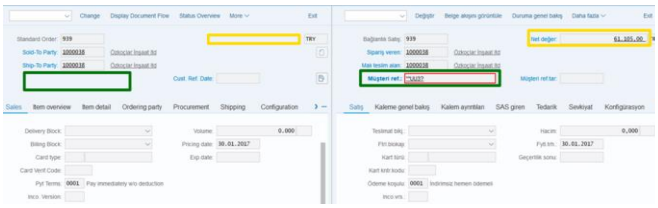
- *Alanı Veri Girişine Kapama / Only-Display field*
- *Alan Gizleme / Hide field*
- *Zorunlu Giriş /Mandatory field*
- *Alan Maskeleme / Mask field*

1. *Girişe Kapama*

Seçilecek kullanıcılar için belirlenen alanlara veri girişi engellenebilir. Değişikliğe açık bir ekranda bir alanın değişikliğe kapatılarak sadece görüntülenebilir olması sağlanabilir.

2. *Alan Gizleme*

Kurallar dahilinde, herhangi bir alan belirlenen roller ve kişiler için ekranda görünmez hale getirilebilir. Şekil 2'de alan gizleme fonksiyonunun örneği görüntüsü sunulmuştur.



Şekil 2. Alan gizleme ekran görüntüleri

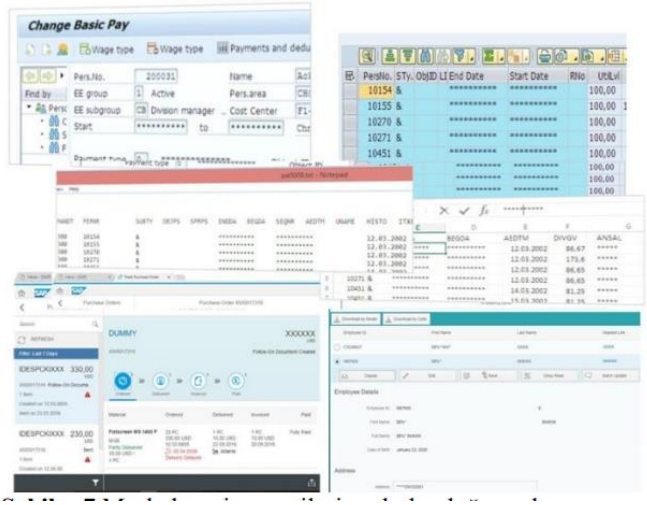
3. *Zorunlu Giriş*

Belirlenen roller veya kişiler için SAP alanlarının doldurulması zorunlu kılınabilir.

4. *Alan Maskeleme*

SAP sisteminin bir bileşeni olan UI Masking ile alan özelinde maskeleme yapılabilmektedir ancak ilgili lisansa sahip olunması gerekir. Eğer lisansına sahip olunursa maskelenmek istenen alanlar için çözümümüz UI masking ile entegre olabilmekte önkoşullarla maskelemeyi yönetebilmektedir. Özellikle Kişisel Verileri Koruma Kanunu'na uyum sağlamak için maskeleme yöntemi çokça tercih edilen bir özellik olmaktadır [5]. Örnek olarak T.C. Kimlik numarasının ilk ve son üç hanesi hariç geri kalan haneler özel karakterlerle gösterilebilmektedir (örn; 111*****111). Maskeleme için gerekli standart işlem kodları ve teknik detaylar [6]'da fazlaca yer almaktadır.

Şekil 3'de bazı işlem kodlarındaki maskeleme örnekleri sunulmuştur.



Şekil 3. Maskelenmiş verilerin bulunduğu ekran görüntüleri

Kişisel verilerin işlenmesi dışında kurumların ticari verilerinin de maskelenmesi yazılım yardımıyla sağlanabilmektedir. Diğer kullanılan veri maskeleme yazılımlarından farklı olarak ekranda bulunan başka bir alanın değerine göre maskeleme kuralları herhangi bir kodlama gerektirmeden uygulanabilmektedir. Maskelenmiş veriler SAP sistemlerinden yazdırılmak istendiğinde ya da yerel dosyalara kaydedilmek istenildiğinde yine diğer yöntemlerden farklı olarak özel karakterlerle maskelenmiş olarak yönlendirilmektedir. Tanımlanan kurallar SAP yetki rollerine aktarılarak sadece belirli kullanıcılar için ilgili alanların görüntülenebilmesi, değiştirilebilmesi ya da tamamen gizlenmesi sağlanabilmektedir.

B. *KAPSAM İÇERİĞİ*

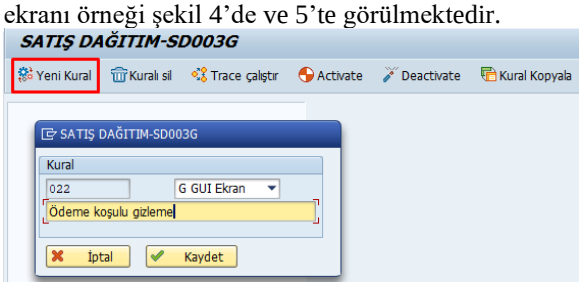
Geliştirilen çözümün içeriğinde temel olarak kapsam şöyle sıralanabilir:

- Kural Oluşturma Ekranı
- Basit ABAP yazılım dili operatörleri kullanılarak Önkoşullar oluşturabilme
- Trace
- Kontrol/Denetim Raporları
- Yetki Raporlar

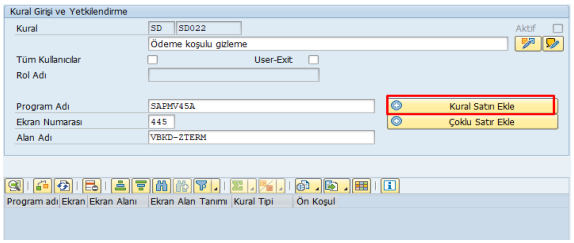
1. *Kural Oluşturma Ekranı*

Bir kural uygulanmak istenen ilgili alanlar belirlendikten sonra, kural oluşturma ekranında yeni kural oluştur denilerek ilgili alan ve alana uygulanmak istenilen davranış (kural tipi) seçilir. Kuralda alan girişi yapılırken alanın teknik bilgileri

referans alınır bunun için, alana ilişkin program adı, ekran alanı ve ekran numarası belirtilerek uygulanacak kural tipi ataması yapılacaktır. SAP sisteminde herhangi bir alan üzerinde F1-F9 yaptığınızda sistem ilgili alanın teknik bilgisini göstermektedir. Buradan faydalanarak kuralda ilgili alana ilişkin teknik bilgiyi girmek son kullanıcı açısından da kolay ve mümkündür. Kural tanımlanırken, ilgili ekran alanı girilip 'kural satırı' olarak eklendikten sonra alana uygulanacak kural tipi seçilir. Bir kural içerisinde birden çok alan girişi yapmak mümkündür ve girilen her bir kural satırı (ekran alanı) için ayrı ayrı kural tipi belirlenebilir.
Kural oluşturulduktan sonra aktifleştirildiğinde yürürlüğe girer ve sistem ilgili kural için bir 'istisna' rol üretir. Böylece kural, bu istisna role sahip kullanıcılar hariç, tüm kullanıcılar için çalışacaktır. Kural tanımına ilişkin çoklu dil desteği de çözüm içeriğinde yer almakta ve kurallar istenirse örneğin modüler bazda gruplanarak ayrı klasörlerde saklanabilir/raporlanabilmektedir. Kural oluşturma ekranı örneği şekil 4'de ve 5'te görülmektedir.



Şekil 4. Kural oluşturma ekran görüntüsü

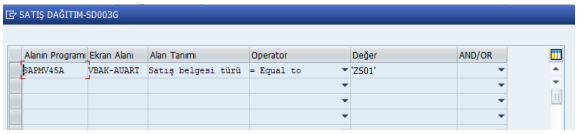


Şekil 5. Kural giriş ve Yetkilendirme ekranı görüntüsü

2. *Önkoşul Oluşturma*

Kuralda belirtilen alanlara ilişkin, kuralın çalışma mantığına bir 'önkoşul' verilmesi çok olası bir durumdur. Başka bir deyişle, bir alanın belirli önkoşullar çerçevesinde (sadece belli bir organizasyonel birim için veya belli bir belge türüne, mal grubuna özel) gizlenmesi veya görüntüleme moduna çekilmesi ihtiyacı olacaktır. İlgili kural satırındaki alanın kural tipine göre denetlenmesini sağlayan bu önkoşullar basit bir şekilde tanımlanabilir. ABAP kodlamasına ihtiyaç duymadan program/alan adı ve değer girilerek ve/veya ile birbiriyle ilişkilendirilebilen önkoşullar ekranda tanımlanabilmektedir. Karşılaştırma operatörleri kullanılarak tekil veya (AND | OR ile bağlayarak) zincirleme koşul tanımlamaları son kullanıcılar tarafından dahi kolaylıkla oluşturulabilir.

Şekil 6'da ön koşul oluşturma ekranı örneği mevcuttur.

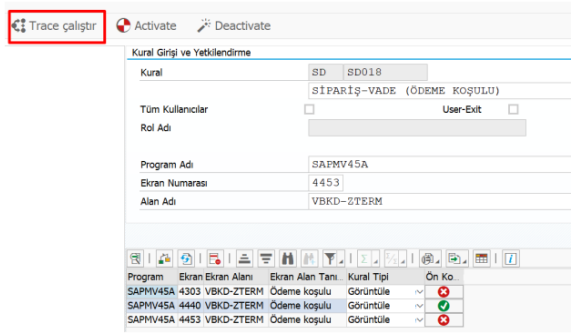


Şekil 6. Ön koşul oluşturma ekran görüntüsü

3. *Trace*

Trace işlevi, aktif kuralların doğru işleyip/işlemediğinin takibini sağlayan bir raporlama imkânı sunar.

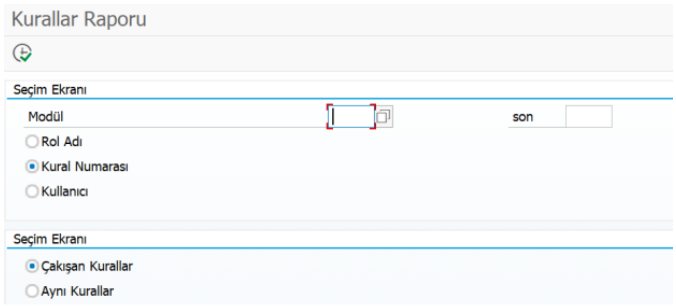
Örnek olarak, kuralda bir ekran alanı için kural tipinde gizleme/hide seçimi yapıldı, ardından trace çalıştır butonu tıklandı ve ilgili ekrana girildikten sonra ekranın ilgili alanı gizlediği görüldü. Geri dönüp trace durdur butonuna tıklanır, neden ilgili alanın gizli göründüğü tanımlanır. Eğer alan gizle kural tipine rağmen gizlenmiyor ise, ya belli bir ön koşul bağlanmış ve bu önkoşul sağlanmadığı için gizlenmemiş olabilir veya ilgili rol kullanıcıya atanmış olduğu için alan ekrana geliyor olabilir. Bu bilgiler trace tarafından raporlanır. Trace, böylece, seçilen kural tiplerine göre yetkilendirmeleri doğru yönetebilecek bir denetim işlevi sağlar. Trace kullanıcı bazında çalışmaktadır. İlgili kullanıcının, ekranın ilgili alanını neden gizli, maskeli, görüntüleme veya edit modunda gördüğünü kısa ve teknik tanımlar ile açıklar. Şekil 7'de örnek bir ekran sunulmaktadır.



Şekil 7. Trace işlevinin görüldüğü ekran görüntüsü

4. *Kontrol/Denetim*

Kurallar oluşturulduktan sonra, sistemde hangi kuralların tanımlandığı, çakışan veya birbiri ile çelişen kurallar var mı gibi kontrolleri yapabilmek adına raporlanabilmesi önemlidir. Klasör bazında rol adına, kural numarasına veya kullanıcıya göre seçim yapılarak raporlanabilir; böylece oluşturulan kuralların kontrol ve denetimi yapılabilir.
Şekil 8' de kurallar raporu ekran görüntüsü örneği sunulmuştur.



Şekil 8. Kurallar raporunun görüldüğü ekran görüntüsü

4.1 *Çakışan Kurallar*

Bir ekranın aynı alanı için iki farklı kural içerisinde farklı ve birbirine tam zıt olan kural tipleri tanımlanmış ise bu iki kural birbiri ile çakışıyor demektir. Raporun seçim ekranında 'Çakışan Kurallar' sekmesini seçip raporu çalıştırırsanız bu tarz birbiri ile çakışan kuralları listeler.

▪ Kural tipi farklı, rol ataması aynı olan durumlar (rol-rol, istisna rol-istisna rol)

▪ Kural tipi aynı, rol ataması farklı olan durumlar (rol-istisna rol, istisna rol-rol)

4.2 *Aynı Kurallar*

Bir ekranın aynı alanı için iki farklı kural içerisinde birbiri ile tamamen aynı kural tipleri tanımlanmış ise bu iki kural birbiri ile aynı; gereksiz tekrar etmiş demektir. Raporun seçim ekranında 'Aynı Kurallar' sekmesini seçip raporu çalıştırırsanız bu tarz birbiri ile aynı tanımlanmış kural satırlarını içeren kuralları listeler.

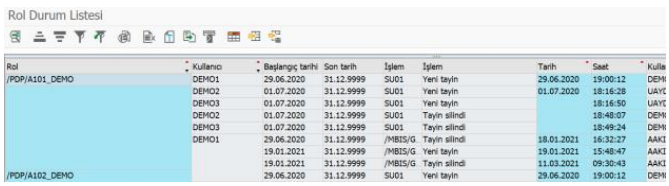
▪ Kural tipi aynı, rol ataması aynı olan durumlar (rol-rol, istisna rol-istisna rol)

▪ Kural tipi farklı, rol ataması farklı olan durumlar (rol-istisna rol, istisna rol-rol)

5. *Raporlama*

Kuralların kontrol ve denetimi dışında, hangi kural için hangi kullanıcıların yetkilendirildiğine dair raporlamalar da elzemdir. Bunun için, rol durum raporunda ilgili kurallara ilişkin oluşturulmuş olan rollerin durumları analiz edilebilmektedir.

Raporun liste ekranında kurallara ilişkin rollerin, hangi tarihte, hangi saatte, hangi kullanıcı tarafından hangi kullanıcıya verildiği (yeni tayin) veya hangi kullanıcıdan alındığı (silindiği) bilgisine ve rolün geçerlilik tarihleri bilgisine ulaşılabilir. Şekil 9'da rapor durum listesi ekran görüntüsü örneği sunulmuştur.



Şekil 9. Rol durum listesi görüldüğü ekran görüntüsü

III. SONUÇ

Uygulamayı geliştirirken SAP sistemini tercih etmemizin nedeni tüm dünyada en yaygın olarak kullanılan iş uygulaması sisteminin gerek kişisel verilerin korunması gerekse şirketlerin veri girişi yaptığı alanların gizliliğinin sağlanmasına yardımcı olmayı hedefleyerek küresel bir çözüme bakış açısı sunmaktır. Geliştirme dili olarak kullanılan ABAP programlama dilinin gerek yaygın kullanım alanına sahip olunması gerek fazla sayıda yazılımcı tarafından bilgi sahibi olunması nedeniyle tercih edilmiştir. Kurumların ticari verilerinin mahremiyetine yönelik olarak da yaygınlaşması öngörülmüştür. Çözüme, makine öğrenmesi teknikleri yardımıyla kullanıcıların yetki kullanım alışkanlıkları öğrenilerek dinamik yetkilendirme önerileri eklenebileceği gibi diğer kurumsal kaynak planlaması yazılımlarına (ERP) veri koruma yaklaşımı getirmesi nedeniyle örnek olacağı düşünülmektedir. Geliştirdiğimiz çözüm yardımıyla SAP kullanan kurumların alan bazlı yetkilendirme ihtiyaçları hem hazır olarak gelen ekranlar hem de kuruma özel geliştirilen ekranlarda sağlanabilmektedir. Fonksiyonel ve organizasyonel rol bazlı yetkilendirmenin sınırlı kaldığı veri koruma ihtiyaçlarında alan bazlı yetkilendirme yöntemi vurgulanarak etkin, verimli ve güvenilir yetki mimarisi sağlanabileceği düşünülmüştür.

IV. TARTIŞMA

Kurumların verileri aynı zamanda ticari sırlarıdır. Bu verilerin kurum dışına her türlü paylaşımı veya sızdırılması kuruma büyük çapta zarar verir. Kurumların bu tür gizli verilerin korunması konusunda büyük çabası vardır. Bu denli önemli ve büyük veriler farklı yazılımlarda tutulur. Bir ERP yazılımı olan SAP'nin kullanıcı yetkilendirme mimarisinin sadece fonksiyonel ve organizasyonel bazda çalışması, daha kapsamlı yetkilendirme ihtiyaçları için yetersiz kalır. Bu duruma karşılık SAP'deki standart yetkilendirme metodu haricinde alan bazlı yetkilendirme işlemini gerçekleştirmek için ek geliştirme yapılması (EXIT) gerekmektedir. Geliştirdiğimiz çözüm, standardın dışına çıkmadan, alan bazlı yetkilendirme fonksiyonunu yönetmek ve daha fazlasını yapmak için bir fikir ve bakış açısı getirmektedir.

V. ANA FİKİR

Bu çalışmada, kurumların veri güvenliğini sağlamak amacıyla ERP sistemlerinde fonksiyonel ve organizasyonel yetkilendirmeye ek olarak alan bazlı yetkilendirme yapabilen ve alan bazlı girişi kapama, gizleme, girişi zorunlu kılma ve maskeli göstermeye fayda sağlayan bir bakış açısı sunulmuştur.

REFERANSLAR

[1] https://dergipark.org.tr/tr/pub/oybd/issue/16333/170999
[2] https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF
[3] https://dergipark.org.tr/tr/pub/ifede/issue/4608/62922
[4] Oğuzhan Atış, Kurumsal Kaynak Planlaması Yazılımlarında Kullanılan Alan Bazlı Yetkilendirme Yöntemlerinin Kişisel Verilerin Korunumu Kanunu Kapsamında Örnek Uygulama Yaklaşımı.
[5] https://www.mbis.com.tr/aura/
[6] Volker Lehnert, Iwona Luther, Björn Christoph, Carsten Pluder, Nicole Fernandes, GDPR and SAP-Data Privacy with SAP Business Suite and SAP S/4HANA,2014.