Pamukkale Univ Muh Bilim Derg, 28(2), 266-276, 2022

Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

# Dağıtık veri tabanı sistemlerinde çok seviyeli güvenlik modeli

## Multi-Level security model in distributed database systems

*Çiğdem BAKIR*[1*], *Mehmet GÜÇLÜ*[1]

[1]Bilgisayar Mühendisliği Bölümü, Elektrik-Elektronik Fakültesi, Yıldız Teknik Üniversitesi, İstanbul, Türkiye.
cigdem.bakr@gmail.com, mehmetguclu007@gmail.com

Geliş Tarihi/Received: 28.01.2021 Düzeltme Tarihi/Revision: 22.06.2021 doi: 10.5505/pajes.2021.69947
Kabul Tarihi/Accepted: 02.07.2021 Araştırma Makalesi/Research Article

**Öz**

*Bilgi güvenliği, bilgiye erişim sağlayarak onu yetkisiz kullanma, değiştirme veya yayma gibi faaliyetleri önleme çabasıdır. Bu, sadece bilginin ele geçirilmesi olarak düşünülmemeli, aynı zamanda bütünlük, erişilebilirlik ve gizlilik gibi unsurların ihlal edilmesinin engellenmesi olarak da değerlendirilmelidir. Bu üç temel unsurdan herhangi birinde oluşan zafiyet, bilgi güvenliğinin ihlali olarak ele alınacaktır. Bu çalışmada, çok seviyeli bir erişim kontrol metodunun geliştirilmesi amacıyla Geliştirilmiş Bell-LaPadula güvenlik modeli dağıtık sistemlere uyarlanmış ve böylece dağıtık veritabanı sistemlerinde bilgi güvenliğinin üç temel unsurundan biri olan gizlilik özelliğinin nasıl sağlandığının gösterilmesi amaçlanmıştır. Çalışmada önerilen geliştirilmiş model, gerçek hayattan alınmış veri kümesi üzerine uygulanmıştır. Önerilen modelin performansı, Rol Tabanlı Erişim Kontrolü ve Geleneksel Erişim Kontrolü modellerinin performansları ile karşılaştırılmıştır. Elde edilen sonuçlar kıyaslandığında, önerilen model ile verilerin daha güvenli ve hızlı bir şekilde kullanıcıların paylaşımına sunulduğu gözlemlenmiştir.*

**Anahtar kelimeler:** Erişim kontrolü, Bell-Lapuda, Güvenlik, Gizlilik.

**Abstract**

*Information security is related with efforts put in to avoid activities such as unauthorized usage, changing or disseminating of information by having access to this information. This should not be only thought as capturing of information but also as avoiding the violation of particulars such as integrity, availability, and confidentiality. Vulnerability that occurs in any one of these three basic elements will be evaluated as violation of information security. In this study, a multi-level access control method was developed. With the model proposed, in addition to the security policies offered by the Bell-LaPadula access control model, a new set of rules was defined and expanded, and a flexible and dynamic access control model was presented. The developed model being proposed in the study has been applied on data cluster which has been obtained from real life. Performance of the proposed model has been compared with the performances of Traditional Access Control models. When the obtained results were compared, it was observed that object access levels were presented more consistently and quickly with the proposed model.*

**Keywords:** Access control, Bell-Lapuda, Security, Confidentilality.

## 1 Giriş

Bilgi güvenliği, bilgiye yetkisiz bir biçimde erişme, kullanma, onu değiştirme, ortadan kaldırma gibi eylemleri önlemek olarak tanımlanır ve gizlilik, bütünlük ve erişilebilirlik olarak adlandırılan belirli temel unsurlardan meydana gelir [1].

Gizlilik, bilginin yetkisiz kişilerce herhangi bir şekilde erişilip okunmasına veya kullanılmasına karşı korunmasıdır. Bütünlük, bilginin yetkisiz kişiler tarafından değiştirilmesinin engellenip orijinalliğinin korunmasıdır. Erişilebilirlik, bilginin ancak yetkili kişilerce ulaşılabilir ve kullanılabilir olmasıdır. Şekil 1'de bilgi güvenliğini sağlamak için bu üç temel unsurlarla korunması gösterilmiştir.

Genel olarak tehditlerin çoğunlukla sistemlerin güvenlik açıklarından ya da zafiyetinden faydalanılarak saldırıya dönüştüğünü, bu tipte saldırıların çalışan sisteme zarar vermesinin önlenmesi için yukarıda bahsedilen güvenlik unsurlarının hepsini birlikte sağlamanın büyük önem taşıdığını söyleyebiliriz. Bu sebeple bir sistem ne kadar güvenli korunuyorsa korunsun burada önemli olan saldırıya mahal verecek unsurları baştan tespit edip gerekli önlemleri almak olmalıdır.

Günümüze kadar birçok uygulama alanına özgü tasarlanmış güvenlik modelinin geliştirildiğini görmekteyiz. Ancak geleneksel güvenlik modelleri, sayısı hızla artan ve gittikçe daha karmaşık hale gelen sistemler üzerinde ihtiyaçları karşılayamamaktadır. Bu durumu ortaya çıkaran faktörler araştırıldığında, özellikle hassas bilgilerin tutulduğu ortamlarda güvenliği sağlamak amacıyla çok sıkı kontrol ve denetimlerin zorunlu kılınmasının, bilgi akış denetiminin tam olarak sağlanamamasının, verilerin güvenli ve hızlı bir şekilde paylaşılamamasının ve uygulama alanında esnekliğin çok büyük oranda yitirilmesinin ciddi rolü olduğu gözlenmektedir [2]-[5].




Şekil 1. Bilgi Güvenliğinin üç temel unsuru.

*Figure 1. The three main elements of information security.*

[*]Yazışılan yazar/Corresponding author

Bu çalışmada, gerçek sistem uygulamalarında geleneksel güvenlik modellerinin zayıf noktaları göz önünde bulundurularak daha işlevsel ve uygulanabilir bir erişim kontrol modeli geliştirilmiştir. Çalışmanın bilimsel katkısı olarak, Bell-LaPadula modelinin sunduğu güvenlik politikalarına ek olarak yeni ve çok seviyeli erişim kontrol prosedürleri tanımlanmıştır. Ayrıca önerdiğimiz model dağıtık veritabanı sistemlerine uyarlanmıştır. Özellikle dağıtık veritabanı sistemlerinde verinin gizlilik unsurunun sağlanması noktasında geliştirilmiş modelin daha esnek ve etkin bir şekilde gerçek sistemlere uyarlanabilmesi amaçlanmıştır.

Bu çalışmanın geri kalan kısmı şu şekilde organize edilmiştir: 2. bölümde ilgili çalışmalar, 3. bölümde dağıtık veritabanı ve güvenlik modeli, 4. Bölümde önerilen çok seviyeli geliştirilmiş güvenlik modelini dağıtık sistemlere yayma, 5. bölümde deneysel çalışma ve 6. bölümde değerlendirme ve sonuç yer alacaktır.

## 2 İlgili çalışmalar

Birçok çalışmada, veritabanlarındaki ve özellikle dağıtık veritabanlarındaki güvenlik endişeleri ele alınmıştır [1],[2], [6]-[9]. Özellikle bazı çalışmalarda her iki sistemde bulunan güvenlik problemleri ayrı ayrı incelenerek güvenlik açısından her bir sistemin zayıf noktaları üzerinde durulmuştur. Bu çalışmalarda, dağıtık veritabanı sistemlerinin, çok seviyeli erişim kontrolü, gizlilik, güvenirlik, bütünlük ve kurtarma gibi birçok güvenlik problemleri ile karşı karşıya kaldığı vurgulanmıştır [5]-[12].

Naeem ve arkadaşları [13], ortak paylaşımı artırmak ve kullanıcıların kişisel bilgilerinin gizliliğini artırmak için takım tabanlı erişim kontrol (TMAC) modeli ile genişletilmiş rol tabanlı erişim kontrol (RBAC) modelini kullanmışlardır. Çalışmada gizlilik, paylaşım ve kural temelli metrikler kullanılarak erişim kontrolü ve gizlilik konuları ile ilgili her iki model karşılaştırılmış ve sağladıkları sonuçlar değerlendirilmiştir.

Bir diğer çalışmada [7], gizliliğin korunması ve genişletilmiş rol tabanlı erişim kontrol (RBAC) güvenlik modeli ile ilgili güvenlik gereksinimleri incelenmiştir. Güvenli sağlık hizmetini desteklemek için sağlık hizmeti entegrasyon platformu (u-HCSIP) tasarlanmış ve bu tasarıma RBAC tabanlı güvenlik modeli uygulanmıştır. İş akışı analiz edilerek önerilen RBAC tabanlı u-HCSIP'in kullanışlılığı doğrulanmıştır.

Dağıtık ortamların özel gereksinimleri gözetilerek erişim kontrolü için tasarlanmış modellerde mevcuttur [8],[14]. Bertolissi ve Fernandez [14] çalışmalarında, her biri kendi kaynaklarını koruyacak şekilde birkaç siteden oluşan bir dağıtılmış sistem üzerine her bir üye tarafından belirtilen yerel politikaları göz önüne alan erişim kontrol politikalarının uygulanması için bir çerçeve önermiştir. Bu çalışma kapsam olarak bizim çalışmamız ile benzerlik göstermektedir. Ancak bizim çalışmamızda, rol tabanlı sistem (kullanıcı grupları) yerine, kaynak ve kullanıcılar sınıflandırılmakta ve siteler arası protokol ile yetki genişlemesi/tanımlaması yapılmaktadır.

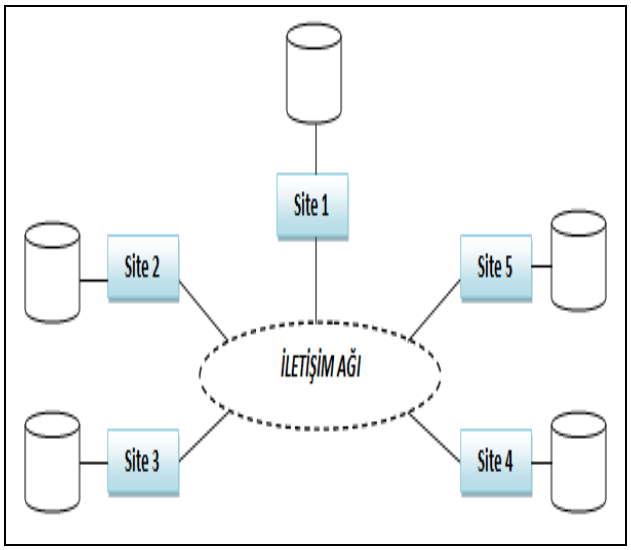
Dasgupta ve arkadaşları [15], önerdikleri metodoloji ile ilk önce çalışanlar arasındaki karşılıklı ilişkilere ve bir organizasyon içindeki rollerine dayalı bir erişim kontrol grafiği oluşturmuştur. Ardından, belirli bir zamanda bir kullanıcının erişim isteğini onaylamasına izin verilen bir dizi izin mekanizması geliştirilmiştir. Önerilen çok kullanıcılı izin stratejisi, iki ampirik veri kümesiyle değerlendirilir ve rapor edilen sonuçlar, farklı kurumsal ve çevresel kısıtlamalar altında bir kullanıcı erişimi için tekrarlamayan onaylayıcıları seçme yeteneğini gösterir.

Davetsiz misafirlerin kovanlarına girmesini engelleyen bal arısının bu davranışı ele alınarak bulut ortamında bir erişim kontrol mekanizması tasarlanmıştır. Çalışmada, bal arısı davranışından ilham alınarak geliştirilmiş Bell-Lapadula Modeli üzerinden bulut güvenliği için yeni bir Öznitelik Esaslı Erişim Kontrolü getirilmiştir [16].

## 3 Dağıtık veritabani ve güvenlik modeli

### 3.1 Dağıtık veritabanı

Biri diğerine mantıksal olarak bağlı verilerin farklı sunucular üzerinde dağıtılmış olmasına rağmen, sunucuların kendi aralarında iletişim ve eşgüdüm içinde çalışarak kullanıcılara tek bir sistem gibi hizmet verebilen sistemlere *dağıtık veritabanı sistemi* diyoruz [17]-[19]. Şekil 2'de görülen saklama birimlerinin her biri birer bilgisayar olabilir ve bu bilgisayarlar aynı ortamda bulunabileceği gibi, bilgisayar ağı ile haberleşen uzak noktalarda konumlanmış da olabilirler. Erişilen verinin hangi birimde saklandığı erişen istemci tarafından bilinmez.




Şekil 2. Dağıtık veritabanını barındıran sunucular.

*Figure 2. Servers hosting the distributed database.*

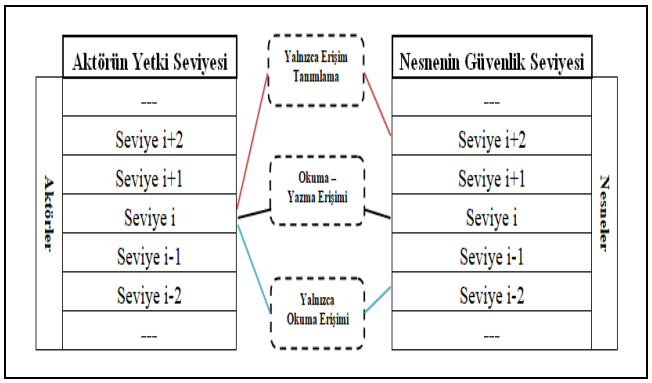
Dağıtık veritabanı sistemlerinin iki türü tanımlanabilir: homojen veritabanı sistemi ve heterojen veritabanı sistemi [18].

### 3.2 Güvenlik modelleri

*Rol Tabanlı Erişim Kontrol Modeli:* Kullanıcıların bir organizasyon içerisindeki görev ve sorumluluklarına göre roller tanımlanır ve kaynaklara erişim yetkisi ve sınırı bu rollere göre şekillendirilir [10]. Kullanıcılar kendilerine tanımlanan rollere göre birtakım yetkilere sahip olur. Bu modelde kullanıcıların görevleri ile ilişkilendirilmiş rolleri sayesinde, 'X kullanıcısı Y nesnesi üzerinde okuma ve yazma yetkilerine sahiptir' yerine 'İnsan Kaynakları Uzmanı personel özlük dosyalarını görüntüler' şeklinde ifadelerin kullanılabilmesine olanak sağlanır. Roller, görevler ile sınırlandırılmış olduğundan modelde "en az yetki" prensibi uygulanır. *Geleneksel Erişim Kontrol Modeli:* Geleneksel erişim kontrol modeli, 'zorunlu erişim kontrolü' ve 'isteğe bağlı erişim kontrolü' olarak ikiye ayrılır. *Zorunlu Erişim Kontrol Modelinde*, kullanıcıların kaynaklara erişimleri merkezi otorite tarafından önceden belirlenmiş birtakım kurallara göre kontrol edilir [10].

Bu tür erişim kontrolü askeri gizlilik sınıflandırmalarında yaygın olarak görülür. *İsteğe Bağlı Erişim Kontrol Modelinde*, kullanıcılar kendilerine verilmiş sınırlar dâhilinde diğer kullanıcılara erişim yetkileri verebilir ya da sınırlamalar getirebilir. Bu tür erişim kontrolü de yaygın olarak işletim sistemlerinin klasör ve dosya yetkilendirmelerinde görülür [10]. *Bell-LaPadula Modeli: Özneler*, güvenlik konusundaki kullanıcıları ve sistemleri ifade etmektedir [20],[21]. Bu çalışmada özneler ise, kullanıcı veya aktör olarak ifade edilmiştir. *Nesneler*, üzerinde okuma, yazma, silme, güncelleme, gibi işlemlerin yapılabildiği her türlü kaynak veriyi ifade etmektedir [21]. Her bir nesne ve aktör için belirli bir güvenlik seviyesi tanımlanmıştır. Aktör hangi güvenlik seviyesinde tanımlanmış ise o güvenlik seviyesinde bulunan nesneler üzerinde tanımlanmış işlemleri gerçekleştirebilir.

Birden fazla güvenlik düzeyinin tanımlandığı model, çeşitli işletim sistemlerinde gizliliği sağlamak için kullanıldığı gibi özellikle güvenlikle ilgili kamu kurumlarında ve askeri uygulamalarda da erişim kontrolünün sağlanabilmesi için kullanılması zorunlu erişim modeli olarak ortaya çıkmaktadır [22]. Modelde varlıklar, aktör ve nesne olmak üzere iki tür sınıftan oluşmaktadır. Aktörlerin yüksek düzeyde güvenlik gerektiren nesnelere yetkisiz erişim sağlamalarının ve güvenlik ihlallerinin önlenmesi amaçlanır. Varlıkları kategorize etmek için sıkça karşılaştığımız hiyerarşik sınıflama metotları kullanılır ve varlıklar güvenlik sınıfları ile nitelendirilir. Örnek olarak varlıkları sınıflamak için kozmik, çok gizli, gizli, sıradan gibi güvenlik sınıfları tanımlanmıştır. Yani sistem içerisindeki her bir varlığın bir güvenlik etiketi mevcuttur. Model, aktörün güvenlik sınıfına göre hangi nesneye hangi yetkileri olduğunu ve hangi işlemleri gerçekleştirebileceğini söyler [22].




Şekil 3. Aktör, nesne ve bu ikili arasındaki erişim yetkileri.

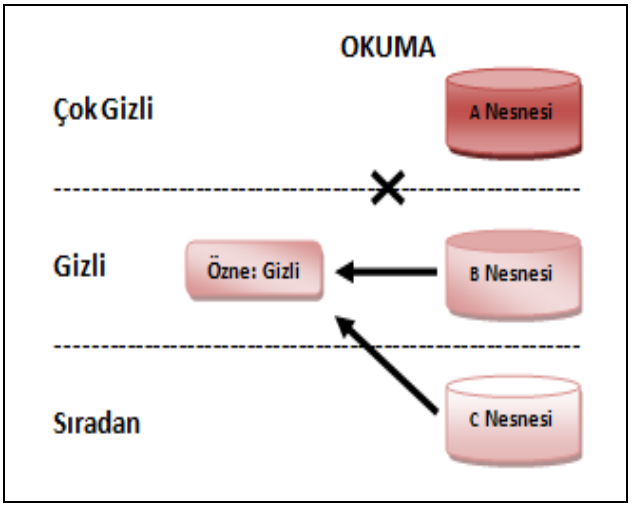
*Figure 3. Access authorizations between the actor and the object.*

Şekil 3'te modeldeki aktörlerin nesneler üzerindeki yetkileri gösterilmektedir. Bu şekil ile kullanıcıların, sınıflandırılmış nesneler üzerinde erişim hakları ve yetkileri ifade edilmektedir. Başka bir deyişle bir aktör, kendi seviyesindeki nesne üzerinde okuma ve yazma işlemlerini yapabilirken, kendi güvenlik seviyesinin altında bulunan nesne üzerinde sadece okuma işlemlerini yapabilir (hiyerarşide yukarıya doğru giden bir raporun bütünlüğünü koruma) [23]. Buna ilaveten, bir aktör kendi güvenlik seviyesinin üstünde bulunan nesnelere ise sadece ekleme işlemlerini yapabilmektedir (bir talimatı değiştirememe, ancak dağıtım yerleri ekleme gibi).

*Tanım*: A= $a_1, a_2, a_{3,...,}a_n$} aktör kümesi, O= {$o_1, o_2, o_3,...,o_m$} nesne kümesi olsun. İki varlık *u* ve *v*, birleşim kümesinden seçilmiş herhangi iki varlık olsun ($u,v \in$A U O). Eğer bir varlığın güvenlik seviyesini gs() fonksiyonu ile ifade edersek: $gs(u) > gs(v)$ ise, varlık *u*, varlık *v* 'ye *baskındır* diyoruz. Bell-LaPadula modelinin sunduğu çeşitli güvenlik politikalarına ve aktör veya nesnenin yer alacağı güvenlik sınıflarına aşağıda değinilmiştir.

### 3.3 Güvenlik politikaları

*Basit Güvenlik Özelliği (Simple Security Property)*: Bir aktör, yüksek hassasiyete sahip nesneler üzerinde okuma işlemi yapamaz [24]. Bir aktör, ancak kendi güvenlik seviyesinde ve kendi güvenlik seviyesinin altında yer alan nesneler üzerinde okuma işlemini gerçekleştirebilir (Şekil 4).

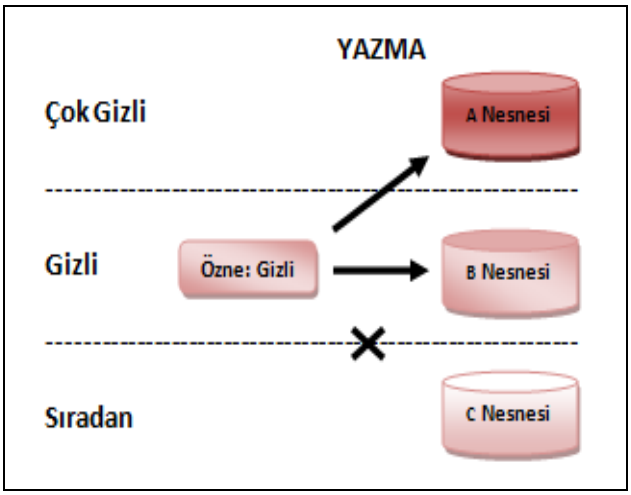



Şekil 4. Basit güvenlik özelliği.

*Figure 4. Simple security feature.*

Basit güvenlik özelliği, *Yukarıdan Okuma Yok (No Read Up)* kuralı şeklinde de ifade edilir [24]. Bir aktör ancak, güvenlik sınıfına baskın olduğu veya aynı seviyede bulunduğu nesneleri okuyabilir (Şekil 7). Ancak nesne aktöre baskın ise okuma yapılamaz. Örneğin, sıradan personel gizli düzeydeki verileri okuyamaz.

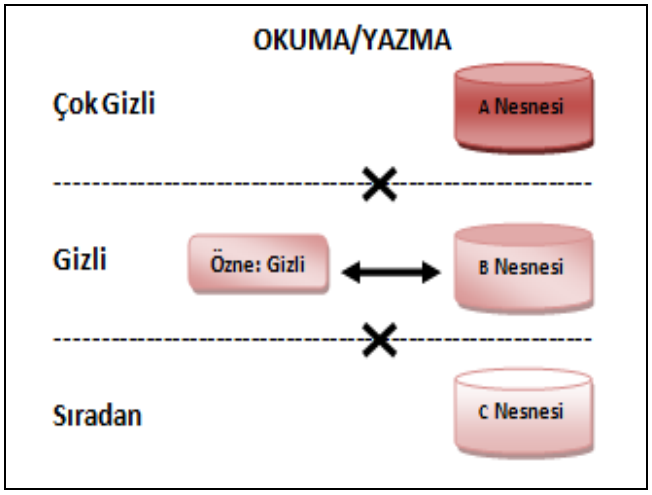
*Yıldız Özelliği (Star Property)*: Bir aktör, düşük hassasiyete sahip nesneler üzerinde yazma işlemi yapamaz [24]. Bir aktör, ancak kendi güvenlik seviyesinde ve kendi güvenlik seviyesinin üzerinde yer alan nesneler üzerinde yazma işlemini gerçekleştirebilir (Şekil 5).




Şekil 5. Yıldız özelliği.

*Figure 5. Star feature.*

Yıldız özelliği, *Aşağıya Yazma Yok (No Write Down)* kuralı şeklinde de ifade edilir [25]. Bir aktör, ancak kendi güvenlik sınıfına baskın olan veya aynı seviyede bulunduğu nesnelere yazabilir (Şekil 11). Ancak aktör nesneye baskın ise yazma yapılamaz. Örneğin, kozmik veriler sıradan (aktörlerin okuyabileceği) dosyalara yazılamaz. *Güçlü Yıldız Özelliği (Strong Star Property)*: Bir aktör, hem düşük hem de yüksek hassasiyete sahip nesneler üzerinde hem okuma hem de yazma işlemlerini yapamaz [24]. Bir aktör, ancak kendi güvenlik seviyesinde yer alan nesneler üzerinde okuma ve yazma işlemlerini gerçekleştirebilir (Şekil 6).




Şekil 6. Güçlü yıldız özelliği.

*Figure 6. Strong star feature.*

### 3.4 Güvenlik Sınıfları

Bir aktör veya nesnenin bulunabileceği güvenlik sınıfları, onun güvenlik seviyesini belirtir. Sınıflandırmada yer alan seviyeler: Kozmik (Top Secret), Çok Gizli (Secret), Gizli (Confidental), Sıradan (Unclassified).

Okuma işlemi, aktörün ancak kendi seviyesi ve altındaki nesneler içindir. Yazma işlemi ise aktörün ancak kendi seviyesi ve üstündeki nesneler içindir. Bu demektir ki aktör kendi seviyesindeki bir nesneyi hem okuyabilir hem de yazabilir.



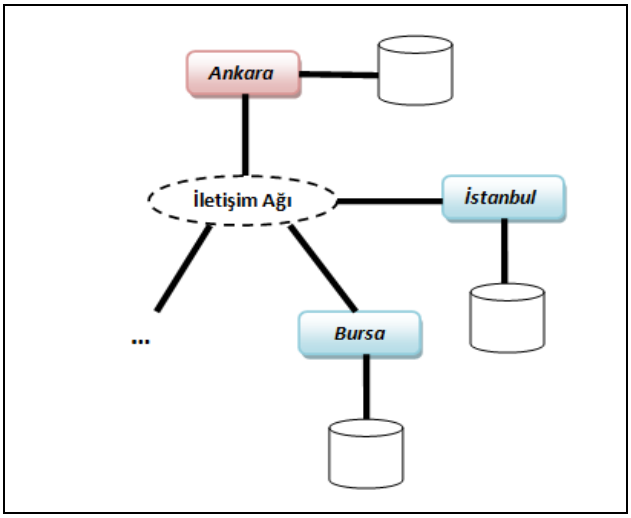

Şekil 7. Güvenlik seviyeleri.

*Figure 7. Security levels.*

Bu güvenlik politikaları gerçekleştirildiğinde, hassas bilgilerin daha düşük düzeydeki nesnelere geçmesi engellenmiş olacak ve bu yolla gizlilik de sağlanmış olacaktır [26]-[30]. Aynı şekilde bulgu veya deneysel sonuçlarda hiyerarşide yukarıya doğru giderken değiştirilmesi veya ekleme yapılması engellenecektir.

## 4 Önerilen model

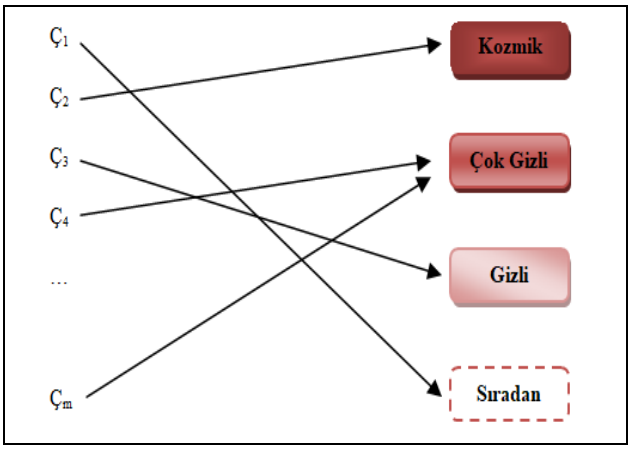
Bu bölümde Önerilen Genişletilmiş Güvenlik Modelimizi dağıtık veritabanlarına uygulayarak verinin gizlilik özelliğinin dağıtık sistemlerde de sağlanması yönündeki adımları gerçekleştirmiş olacağız. Şekil 8'de bir kurumun farklı şehirlerde bulunan şubelerindeki veritabanları gösterilmektedir. Bir şubenin kendi nezdinde tuttuğu veritabanında saklı nesneler üzerinde okuma ve yazma (read/write) işlemlerinin yürütülebilmesi durumu, o şubedeki çalışanlara verilen hak ve yetkiler ile sınırlandırılmıştır.




Şekil 8. Bir kurumun dağıtılmış veritabanlarının konumu.

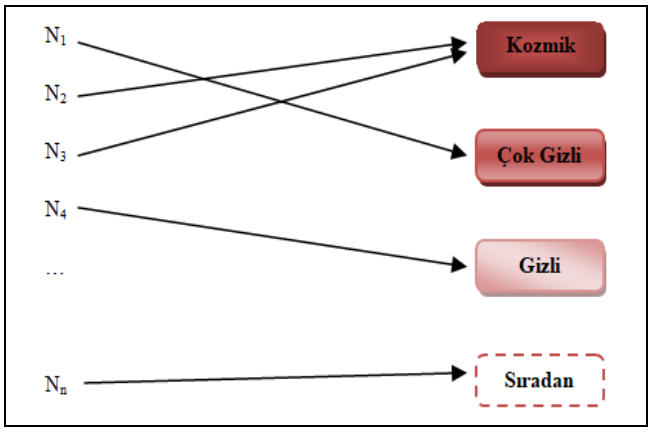
*Figure 8. Location of an organization's distributed databases.*

Şekil 8'de örneğin İstanbul, Bursa, vs. bir güvenlik kurumunun şubeleri ve Ankara ise merkez birimi olsun. Bir şubedeki her çalışana pozisyonuna bağlı olarak bir güvenlik seviye ataması yapılır (Şekil 9). Yine her şube nezdinde tutulan veritabanında saklı nesneler vardır ve bu veritabanında saklı nesnelere de bir güvenlik seviye ataması yapılır (Şekil 10). Güvenlik seviyesi ise 4 kategoride toplanır: *Kozmik, Çok Gizli, Gizli, Sıradan.* Şirketin şube çalışanları $Ç=\{Ç_1,Ç_2,...,Ç_m\}$ ve nesneler $N=\{N_1,N_2,...,N_n\}$ kümesinde gösterilmiştir.




Şekil 9. Çalışanlara güvenlik seviyesi atama.

*Figure 9. Assign a security level to employees.*




Şekil 10. Nesnelere güvenlik seviyesi atama.

*Figure 10. Assign a security level to objects.*

### 4.1 Senaryolar

x ve y, sırasıyla Ç ve N kümelerinden seçilmiş herhangi iki varlığı ifade etmektedir. Okuma (Read) ve Yazma (Write) işlemleri R ve W sembollerini ve G() fonksiyonu ise güvenlik seviyesini belirtmektedir.

***Senaryo 1 (S1):*** Her şube çalışanı, kendi güvenlik seviyesiyle eşdeğer olan veya altında yer alan güvenlik seviyesine atanmış nesneler üzerinde yalnızca okuma işlemini gerçekleştirebilir (Basit Güvenlik Özelliği) [24]. Yani bir çalışanın ( $Ç_x$) güvenlik seviyesi erişim sağladığı nesnenin ($N_y$) güvenlik seviyesine eşit veya altında ise çalışan bu nesneyi görüntüleyebilir (Şekil 8).

$$G(X) \leq G(Y \Rightarrow \text{Yetki[x]} = \{R\}_y \quad (1)$$

***Senaryo 2 (S2):*** Her şube çalışanı, kendi güvenlik seviyesiyle eşdeğer olan veya üzerinde yer alan güvenlik seviyesine atanmış nesneler üzerinde yalnızca yazma işlemini gerçekleştirebilir (Yıldız Özelliği) [24]. Yani bir çalışanın ($Ç_x$) güvenlik seviyesi erişim sağladığı nesnenin ($N_y$) güvenlik seviyesine eşit veya üzerinde ise çalışan bu nesne üzerinde işlem yapabilir (Şekil 9).

$$G(X) \geq G(Y) \Rightarrow \text{Yetki[x]} = \{W\}_y \quad (2)$$

***Senaryo 3 (S3):*** Her şube çalışanı, kendi güvenlik seviyesiyle eşdeğer olan güvenlik seviyesine atanmış nesneler üzerinde okuma ve yazma işlemlerini birlikte gerçekleştirebilir (Güçlü Yıldız Özelliği) [24]. Yani bir çalışanın ($Ç_x$) güvenlik seviyesi erişim sağladığı nesnenin ($N_y$) güvenlik seviyesine eşit ise çalışan bu nesneyi görüntüleyebilir ve nesne üzerinde işlem yapabilir (Şekil 10).

$$G(X) = G(Y) \Rightarrow \text{Yetki[x]} = \{R, W\}_y \quad (3)$$

### 4.2 Özel hak ve yetkiler

Herhangi bir özel düzenleme yapılmadığında bir şube çalışanı, başka bir şubeye ait nesneler üzerinde işlem yapma yetkisine sahip değildir (Örneğin Bursa çalışanının İstanbul nesnelerine erişememesi gibi). Ancak, merkez birim tarafından yetkilendirilmek suretiyle veya iki birim arası anlaşma (protokol) ile bir şube çalışanı diğer şubede de birtakım haklara sahip olabilir. Tablo 1'de şubelere göre çalışanların yetki seviyeleri gösterilmektedir. Ankara biriminde çalışanlar güvenlik seviyesine göre A1 (Ankara Kozmik), A2 (Ankara Çok Gizli), A3 (Ankara Gizli) ve A4 (Ankara Sıradan), İstanbul şubesinde çalışanlar güvenlik seviyesine göre İ1 (İstanbul Kozmik), İ2 (İstanbul Çok Gizli), İ3 (İstanbul Gizli) ve İ4 (İstanbul Sıradan) ve Bursa şubesinde çalışanlar güvenlik seviyesine göre B1 (Bursa Kozmik), B2 (Bursa Çok Gizli), B3 (Bursa Gizli) ve B4 (Bursa Sıradan) gruplarında toplanmıştır.

***Özel Durum 1 (Ö1: Merkez-Şube arası):*** Merkez birimi diğer şubeler üzerinde merkezdeki aynı yetkiye sahiptir (güvenlik seviyesi olarak aynı düzeydedir). Bu doğrultuda bir merkez çalışanı, ait olduğu güvenlik seviyesiyle eşdeğer olan güvenlik seviyesine ait tüm şube çalışanlarının sahip olduğu hak ve yetkiye sahiptir.

Tablo 1'de Ankara'nın merkez birim olması sebebiyle bu birim çalışanlarının tamamı, güvenlik düzeyine denk gelen diğer şube çalışanlarının toplandığı grupta ayrıca yer aldığı görülmektedir.

Tablo 1. Özel durum 1'e göre oluşan yeni yetki seviyeleri.

*Table 1. New authorization levels according to special case 1.*

| | Ankara | İstanbul | Bursa |
|---|---|---|---|
| Kozmik | A1 | İ1, A1 | B1, A1 |
| Çok Gizli | A2 | İ2, A2 | B2, A2 |
| Gizli | A3 | İ3, A3 | B3, A3 |
| Sıradan | A4 | İ4, A4 | B4, A4 |

***Özel Durum 2 (Ö2: Şube - Şube arası):*** Merkez birim tarafından yetkilendirilmek suretiyle veya protokol ile herhangi bir şube çalışanı, ait olduğu güvenlik seviyesiyle eşdeğer olan güvenlik seviyesine ait başka bir şube çalışanının sahip olduğu hak ve yetkiye sahiptir. (Örneğin İstanbul çalışanı k, Bursa çalışanı i olsun. G(i) = G(k) ise k, i'nin yetkilerine sahip olabilir).

Tablo 2'de İstanbul Kozmik (İ1) grubunda yer alan bir şube çalışanının ($İ1_k$) Ö2'den dolayı Bursa Kozmik (İ1) grubunda da yer aldığı görülmektedir.

Tablo 2. Özel durum 2 'e göre oluşan yeni yetki seviyeleri

*Table 2. New authorization levels according to special case 2.*

| | Ankara | İstanbul | Bursa |
|---|---|---|---|
| *Kozmik* | A1 | İ1, A1 | B1, A1, $İ1_k$ |
| *Çok Gizli* | A2 | İ2, A2 | B2, A2 |
| *Gizli* | A3 | İ3, A3 | B3, A3 |
| *Sıradan* | A4 | İ4, A4 | B4, A4 |

***Özel Durum 3 (Ö3: Şube-Şube arası, Kıdem Farkı):*** Merkez birim tarafından yetkilendirilmek suretiyle veya iki birim arası anlaşma ile herhangi bir şube çalışanı, ait olduğu güvenlik seviyesinin altında yer alan güvenlik seviyesine ait başka bir şube çalışanının sahip olduğu hak ve yetkiye sahiptir. (Örneğin Bursa çalışanı z, İstanbul çalışanı y olsun. G(z) > G(y) ise z, y'nin yetkilerine sahip olabilir.)

Tablo 3'te Bursa Gizli (B3) grubunda yer alan bir şube çalışanının ($B3_z$) Ö3'ten dolayı İstanbul Sıradan (İ4) grubunda da yer aldığı görülmektedir.

Tablo 3. Özel durum 3'e göre oluşan yeni yetki seviyeleri.

*Table 3. New authorization levels according to special case 3.*

| | Ankara | İstanbul | Bursa |
|---|---|---|---|
| *Kozmik* | A1 | İ1, A1 | B1, A1 |
| *Çok Gizli* | A2 | İ2, A2 | B2, A2 |
| *Gizli* | A3 | İ3, A3 | B3, A3 |
| *Sıradan* | A4 | İ4, A4, $B3_z$ | B4, A4 |

***Özel Durum 4 (Ö4: Şube-Şube arası):*** Merkez birim tarafından yetkilendirilmek suretiyle veya iki birim arası anlaşma ile herhangi bir şube çalışanı, ait olduğu güvenlik seviyesinin

üzerinde yer alan güvenlik seviyesine ait başka bir şube çalışanının sahip olduğu hak ve yetkiye sahiptir. (Örneğin İstanbul çalışanı x, Bursa çalışanı t olsun. G(x) < G(t) ise x, t'nin yetkilerine sahip olabilir). Tablo 4'te İstanbul Gizli (İ3) grubunda yer alan bir şube çalışanının ($İ3_x$) Ö4'ten dolayı Bursa Çok Gizli (B2) grubunda da yer aldığı görülmektedir.

Tablo 4. Özel durum 4'e göre oluşan yeni yetki seviyeleri.

*Table 4. New authorization levels according to special case 4.*

| | Ankara | İstanbul | Bursa |
|---|---|---|---|
| *Kozmik* | A1 | İ1, A1 | B1, A1 |
| *Çok Gizli* | A2 | İ2, A2 | B2, A2, $İ3_x$ |
| *Gizli* | A3 | İ3, A3 | B3, A3 |
| *Sıradan* | A4 | İ4, A4 | B4, A4 |

### 4.3 Tanımlanmış kurallara (özel durumlara) göre senaryoların uygulaması

Bir kullanıcı, kendi şubesi dışında özel durum ya da şubeler arası protokol çerçevesinde, bulunduğu şubedeki yetki seviyesinin eşdeğerinde, altında ya da üzerinde bir yetki ile diğer şubelerin yetki listelerinde yer alabilir. Bu durum dikkate alınarak oluşturulan kullanıcı erişim seviyeleri Tablo 5'te gösterilmektedir.

Tablo 5 Kullanıcı erişim seviyesi.

*Table 5. User access level.*

| | Ankara | İstanbul | Bursa |
|---|---|---|---|
| *Kozmik* | A1 | İ1, A1 | B1, A1, $İ1_k$ |
| *Çok Gizli* | A2 | İ2, A2 | B2, A2, $İ3_x$ |
| *Gizli* | A3 | İ3, A3 | B3, A3 |
| *Sıradan* | A4 | İ4, A4, $B3_z$ | B4, A4 |

Merkez birim tarafından yetkilendirilmek suretiyle veya iki birim arası anlaşma ile kullanıcılara atanan özel yetki seviyeleri protokol dosyalarında tutulur. Protokol dosyaları PD sembolü ile ifade edilir. Tablo 5'e göre oluşan protokol dosyalarına Tablo 6 ve Tablo 7'de yer verilmiştir.

Tablo 6. Bursa şubesinde tutulacak protokol dosyası (PD).

*Table 6. Protocol file (PD) to be kept in Bursa branch.*

| İstanbul | Bursa |
|---|---|
| İ1 | B1, $İ1_k$ |
| İ3 | B2, $İ3_x$ |

Tablo 7. İstanbul şubesinde tutulacak protokol dosyası (PD).

*Table 7. Protocol file (PD) to be kept in Istanbul branch.*

| İstanbul | Bursa |
|---|---|
| İ4, $B3_z$ | B4 |

İletişim ağında yer alan her bir kullanıcının şube ya da şubelerdeki yetki seviyeleri belirlendikten sonra her bir şube nezdinde o şubeye ait Kozmik, Çok Gizli, Gizli ve Sıradan güvenlik seviyelerinde erişim sağlayacak kullanıcılar listesi dosyalarda tutulur. Erişim hakları dosyası olarak isimlendirdiğimiz bu dosyalarda bir şubenin her bir güvenlik seviyesine erişim sağlayabilecek kullanıcı ve kullanıcıların bağlı olduğu şube ve o şubedeki güvelik seviyesi bilgileri tutulur. Erişim hakları dosyası E sembolü ile ifade edilir. Her bir şube için oluşturulmuş erişim hakları dosyası Tablo 8, Tablo 9. ve Tablo 10'da gösterilmektedir.

$A_1$, $A_2$, $A_3$ *ve* $A_4$: Ankara birimindeki 1., 2., 3. ve 4. yetki seviyelerini (Kozmik, Çok Gizli, Gizli, Sıradan) temsili olarak gösterir. $A1_1$, $A1_2$, ..., $A1_p$: $A_1$ yetki seviyesindeki tüm kullanıcıları gösterir. $A2_1, A2_2, ..., A2_r$: $A_2$ yetki seviyesindeki tüm kullanıcıları gösterir. $A3_1, A3_2, ..., A3_s$: $A_3$ yetki seviyesindeki tüm kullanıcıları gösterir. $A4_1$, $A4_2$, ..., $A4_u$: $A_4$ yetki seviyesindeki tüm kullanıcıları gösterir.

Tablo 8. Merkez birim nezdinde tutulan kullanıcı erişim hakları dosyası (EA).

*Table 8. User access rights file (EA) held with the central unit.*

| | |
|---|---|
| $A_1$ | $A1_1, A1_2,...,A1_p$ |
| $A_2$ | $A2_1, A2_2,...,A2_r$ |
| $A_3$ | $A3_1, A3_2,...,A3_s$ |
| $A_4$ | $A4_1, A4_2,...,A4_u$ |

Tablo 9. İstanbul şubesi nezdinde tutulan kullanıcı erişim hakları dosyası (Eİ).

*Table 9. User access rights file (EI) held with the Istanbul branch.*

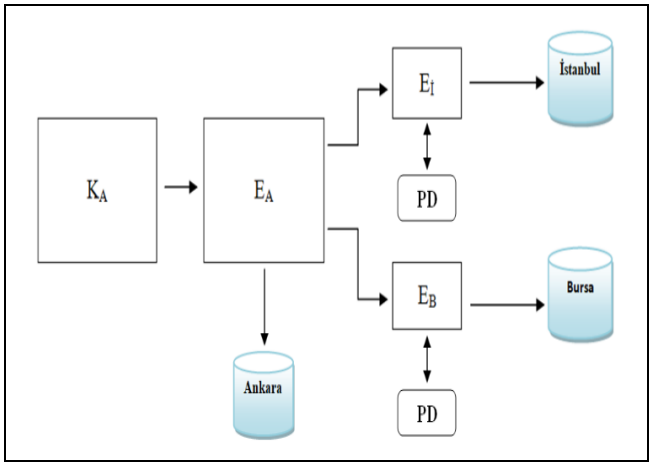
| | |
|---|---|
| $İ_1$ | $İ1_1, İ1_2,...,İ1_a$, A1 |
| $İ_2$ | $İ2_1, İ2_2,...,İ2_b$, A2 |
| $İ_3$ | $İ3_1, İ3_2,...,İ3_c$, A3 |
| $İ_4$ | $İ4_1, İ4_2,...,İ4_d$, A4, $B3_z$ |

Tablo 10. Bursa şubesi nezdinde tutulan kullanıcı erişim hakları dosyası (EB).

*Table 10. User access rights file (EB) held with the Istanbul branch.*

| | |
|---|---|
| $B_1$ | $B1_1, B1_2,...,B1_e$, A1, $İ1_k$ |
| $B_2$ | $B2_1, B2_2,...,B2_f$, A2, $İ3_x$ |
| $B_3$ | $B3_1, B3_2,...,B3_g$, A3 |
| $B_4$ | $B4_1, B4_2,...,B4_h$, A4 |

Ankara biriminde yer alan bir kullanıcının kendi bulunduğu birime erişimleri için yalnızca kendi birimine ait ($E_A$) erişim hakları dosyası kontrol edilirken, farklı bir birime erişimi halinde hem $E_A$ hem de erişim yapmak istediği birim nezdinde tutulan erişim hakları dosyası (İstanbul şubesi için $E_İ$ ve/veya Bursa şubesi için $E_B$) kontrol edilir. Şekil 11'te Ankara birimindeki kullanıcılar için erişim kontrol prosedürü gösterilmiştir. $K_A$: Ankara birimindeki tüm kullanıcıları gösterir.



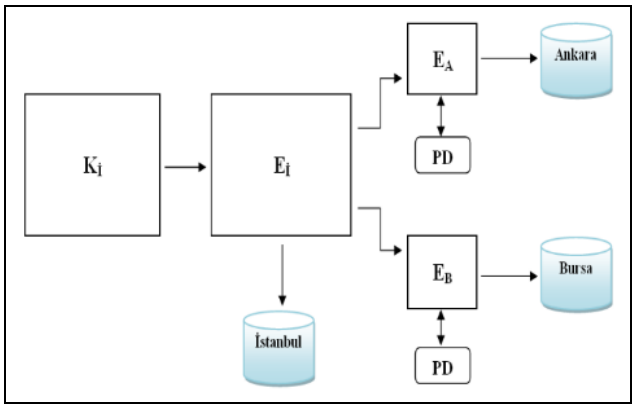

Şekil 11. Ankara birimindeki kullanıcıların erişim kontrol prosedürü.

*Figure 11. Access control procedure of users in Ankara unit.*

Ayrıca erişim hakları dosyasının güncel olup olmadığı protokol dosyalarına bakılarak karar verilir. Şayet protokol dosyası (PD) ile erişim hakları dosyasında (E) çelişen bir yetkilendirme durumu söz konusu olursa kullanıcının erişim talebi yetkisiz

olarak değerlendirilir ve reddedilir. Tersi durumda ise erişim hakları dosyasında kullanıcı için tanımlanmış bir yetki var ise ve bu yetki protokol dosyası ile destekleniyor ise, kullanıcı o şubenin ilgili yetki seviyesine erişim yapabilir. Bu kontrol mekanizması tüm şubeler için geçerlidir. *İ1, İ2, İ3 ve İ4*: İstanbul şubesindeki 1., 2., 3. ve 4. yetki seviyelerini (Kozmik, Çok Gizli, Gizli, Sıradan) temsili olarak gösterir. *İ1$_1$, İ1$_2$, ..., İ1$_a$, A1*: $İ_1$ yetki seviyesindeki tüm kullanıcıları gösterir. *İ2$_1$, İ2$_2$, ..., İ2$_b$, A2*: $İ_2$ yetki seviyesindeki tüm kullanıcıları gösterir. *İ3$_1$, İ3$_2$, ..., İ3$_c$, A3*: $İ_3$ yetki seviyesindeki tüm kullanıcıları gösterir. *İ4$_1$, İ4$_2$, ..., İ4$_d$, A4, B3$_2$*: $İ_4$ yetki seviyesindeki tüm kullanıcıları gösterir.

İstanbul şubesinde yer alan bir kullanıcının kendi bulunduğu birime erişimleri için yalnızca $E_İ$ erişim hakları dosyası kontrol edilirken, farklı bir birime erişimi halinde hem $E_İ$ hem de erişim yapmak istediği birim nezdinde tutulan erişim hakları dosyası (Ankara birimi için $E_A$ veya Bursa şubesi için $E_B$) kontrol edilir. Şekil 12'de İstanbul şubesindeki kullanıcılar için erişim kontrol prosedürü gösterilmiştir. $K_İ$: İstanbul şubesindeki tüm kullanıcıları gösterir. *B$_1$, B$_2$, B$_3$ ve B$_4$*: Bursa şubesindeki 1., 2., 3. ve 4. yetki seviyelerini (Kozmik, Çok Gizli, Gizli, Sıradan) temsili olarak gösterir. *B1$_1$, B1$_2$, ..., B1$_e$, A1, İ1$_k$*: $B_1$ yetki seviyesindeki tüm kullanıcıları gösterir. *B2$_1$, B2$_2$, ..., B2$_f$, A2, İ3$_x$*: $B_2$ yetki seviyesindeki tüm kullanıcıları gösterir. *B3$_1$, B3$_2$, ..., B3g, A3*: $B_3$ yetki seviyesindeki tüm kullanıcıları gösterir. *B4$_1$, B4$_2$, ..., B4$_h$, A4*: $B_4$ yetki seviyesindeki tüm kullanıcıları gösterir.

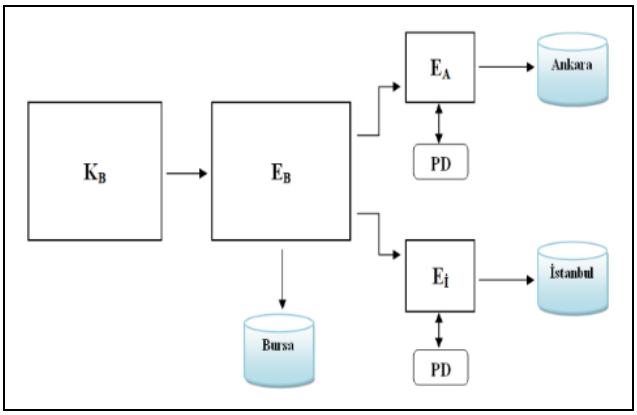



Şekil 12. İstanbul şubesindeki kullanıcıların erişim kontrol prosedürü.

*Figure 12. Access control procedure of users in Istanbul unit.*

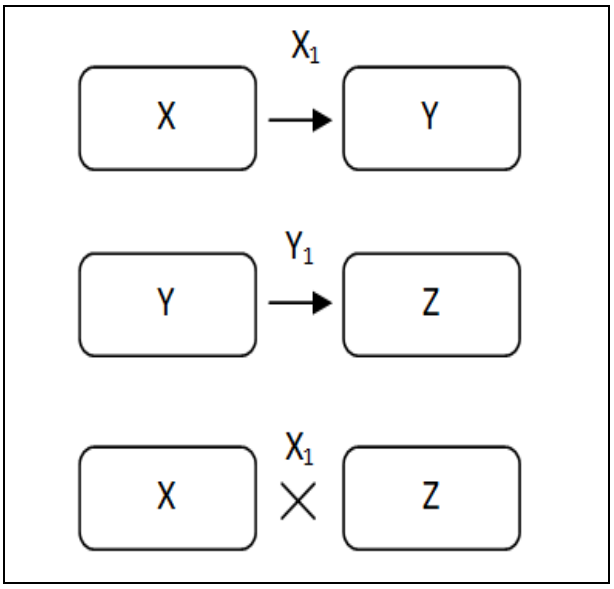
Bursa şubesinde yer alan bir kullanıcının kendi bulunduğu birime erişimleri için yalnızca $E_B$ erişim hakları dosyası kontrol edilirken, farklı bir birime erişimi halinde hem $E_B$ hem de erişim yapmak istediği birim nezdinde tutulan erişim hakları dosyası (Ankara birimi için $E_A$ veya İstanbul şubesi için $E_İ$) kontrol edilir. Şekil 13'te Bursa şubesindeki kullanıcılar için erişim kontrol prosedürü gösterilmiştir. $K_B$: Bursa şubesindeki tüm kullanıcıları gösterir.

Bir birime özel yetkilendirme ya da şubeler arası protokol ile tanınan ayrıcalıklar yalnızca o birimin çalışanları için geçerli olur. Bir başka deyişle, özel protokoller ile başka bir birimde 1., 2., 3. veya 4. seviyelerin birine yetkilendirilen bir kullanıcı, yetkilendirildiği şubede yer alan çalışanların başka bir şube için geçerli olan özel hak ve yetkilerine sahip olamaz. Şekil 14'te gösterildiği gibi X birimindeki bir kullanıcı ($X_1$) Y biriminde bir yetkiye sahip olması neticesinde Y birimine erişim sağlayabildiği, yine Y birimindeki bir kullanıcı ($Y_1$) Z biriminde yetkiye sahip olması neticesinde Z birimine erişim sağlayabildiği, ancak X birimindeki $X_1$ kullanıcısı Y biriminde bir yetkiye sahip olsa da, bu kullanıcı Y birimindeki $Y_1$ kullanıcısının Z birimi için geçerli olan yetkisine sahip olamayacağından $X_1$ kullanıcısının Z birimine erişim yapamayacağını söyleyebiliriz.




Şekil 13. Bursa şubesindeki kullanıcıların erişim kontrol prosedürü.

*Figure 13. Access control procedure of users in Bursa unit.*




Şekil 14. Erişim yetkileri.

*Figure 14. Access authorization.*

Sonuç olarak; yukarıda anlatılan erişim prosedürlerine göre Tablo 5'deki yetki seviyelerini önerilen geliştirilmiş güvenlik modelinin getirdiği güvenlik politikaları kapsamında yorumlayacak olursak;

***Senaryo 1'e göre;***

- *"Kozmik"* güvenlik seviyesindeki İstanbul çalışanı (İ1), İstanbul ve Ö2 kuralından dolayı Bursa şubelerindeki tüm güvenlik seviyelerinde yer alan nesneler üzerinde yalnızca okuma işlemini yapabilmektedir.,
- *"Gizli"* güvenlik seviyesindeki İstanbul çalışanı (İ3), İstanbul şubesindeki *"Gizli" ve "Sıradan"*, Ö4 kuralından dolayı Bursa şubesindeki *"Çok Gizli", "Gizli" ve "Sıradan"* güvenlik seviyelerinde yer alan nesneler üzerinde yalnızca okuma işlemini yapabilmektedir,

- *"Gizli"* güvenlik seviyesindeki Bursa çalışanı (B3), Bursa şubesindeki *"Gizli"* ve *"Sıradan"*, Ö3 kuralından dolayı İstanbul şubesindeki *"Sıradan"* güvenlik seviyelerinde yer alan nesneler üzerinde yalnızca okuma işlemini yapabilmektedir.

***Senaryo 2'ye göre;***

- *"Kozmik"* güvenlik seviyesindeki İstanbul çalışanı (İ1), İstanbul ve Ö2 kuralından dolayı Bursa şubelerindeki *"Kozmik" güvenlik* seviyesinde yer alan nesneler üzerinde yalnızca yazma işlemini yapabilmektedir,
- *"Gizli"* güvenlik seviyesindeki İstanbul çalışanı (İ3), İstanbul şubesindeki *"Gizli"*, *"Çok Gizli"* ve *"Kozmik"*, Ö4 kuralından dolayı Bursa şubesindeki *"Çok Gizli"* ve *"Kozmik"* güvenlik seviyelerinde yer alan nesneler üzerinde yalnızca yazma işlemini yapabilmektedir,
- *"Gizli"* güvenlik seviyesindeki Bursa çalışanı (B3), Bursa şubesindeki *"Gizli"*, *"Çok Gizli"* ve *"Kozmik"*, Ö3 kuralından dolayı İstanbul şubesindeki tüm güvenlik seviyelerinde yer alan nesneler üzerinde yalnızca yazma işlemini yapabilmektedir.

***Senaryo 3'e göre;***

- *"Kozmik"* güvenlik seviyesindeki İstanbul çalışanı (İ1), İstanbul ve Ö2 kuralından dolayı Bursa şubelerindeki *"Kozmik" güvenlik* seviyesinde yer alan nesneler üzerinde hem okuma hem de yazma işlemini yapabilmektedir,
- *"Gizli"* güvenlik seviyesindeki İstanbul çalışanı (İ3), İstanbul şubesindeki *"Gizli"*, Ö4 kuralından dolayı Bursa şubesindeki *"Çok Gizli"* güvenlik seviyelerinde yer alan nesneler üzerinde hem okuma hem de yazma işlemini yapabilmektedir,
- *"Gizli"* güvenlik seviyesindeki Bursa çalışanı (B3), Bursa şubesindeki *"Gizli"*, Ö3 kuralından dolayı İstanbul şubesindeki *"Sıradan"* güvenlik seviyelerinde yer alan nesneler üzerinde hem okuma hem de yazma işlemini yapabilmektedir.

Oluşturduğumuz modelin sözde kodu aşağıdaki gibidir:

```
Algoritma OnerilenModel (E,P)
U←Kullanıcı
O← Nesne
E ←Erişim Dosyası
P← Protokol Dosyası
for i=1 to u
    for j=1 to o
        if (U[i]→O[j])
            if (U[i].EA="Ankara")
                read, write data O[j]
            else if (EA=Pi)
                read, write data O[j]
            else if (EA=PB)
                read, write data O[j]
            else
                don't read, don't write data O[j]
            end if
  end for
end for
```

Bu modelin algoritma karmaşıklığı $Q(n^4)$'tür.

Yukarıda belirtilen senaryoların dışında ortaya çıkabilecek tüm durumlarda, kullanıcıların nesnelere erişebilmesi ve nesneler üzerinde işlem yapabilmesi mümkün değildir. Çünkü kullanıcılara sahip olduğu statü ve rol dışında gereksiz ve/veya aşırı yetki verilmesi veri gizliliği problemini meydana getirir. Ayrıca modele daha esnek bir yapı kazandırılırken bilgi güvenliğinin üç temel unsurunu gözardı etmemek gerekir. Görüldüğü üzere dağıtık veritabanı üzerine kurulu bir sistem için geliştirilmiş önerilen güvenlik modeli sayesinde, modelin sunduğu standart politikalar dağıtık sistemlere uygulanabildiği gibi, özel hak ve yetkilerle donatılmış kullanıcıların mevcut güvenlik seviyelerinin üzerinde yer alan seviyelerdeki nesnelere erişim yapmaları ve aynı zamanda mevcut güvenlik seviyelerinin altında yer alan seviyelere bilgi aktarmaları kontrollü bir şekilde gerçekleştirilebilmektedir.

## 5 Deneysel çalışma

Çalışmada sağlık ve adalet hizmetlerini sağlayan kamu kuruluşlarından alınan gerçek veri setleri kullanılmış, önerilen erişim kontrol modeli ve diğer yöntemlerin başarısı her bir veri setinde elde edilen sonuçlara göre değerlendirilmiştir.

### 5.1 Veri setleri

Çalışmada kullanılan farklı sektörlerden alınmış iki veri seti ön işlemden geçirilerek veri setinde geçen her bir kullanıcı ve nesne güvenlik boyutlarına göre sınıflandırılmıştır. Sınıflandırma işleminde, işletmelerin gerçek sınıflandırma ölçütleri baz alınmıştır. Sağlık sektöründen alınan veri kümesi 430 kullanıcı, 55.300 nesneden ve Yargı sektöründen alınan veri kümesi ise 292 kullanıcı, 72.988 nesneden oluşmaktadır. Veri setleri "Sağlık Veri Seti" ve "Yargı Veri Seti" olarak ifade edilmiştir.

### 5.2 Deneysel analizler

Önerilen modelimiz ile birlikte diğer erişim kontrol modelleri de gerçek bir dağıtık sistem sunan platform üzerinde çalıştırılmış ve tüm modeller iki veri setine ayrı ayrı uygulanmıştır. Her bir veri setine uygulanan tüm modeller için elde edilen erişim düzeyi sonuçları (okuma, yazma, okuma ve yazma, vd.), veri setinin alındığı sektöre ait uygulamada geçen erişim düzeyi sonuçları ile karşılaştırılarak metotların performans değerleri analiz edilmiştir.

Veri kümelerine uygulanan metotların performans değerlendirilmesinde her metodun doğru erişim düzeyi ve erişim hızı tespit yüzdeleri esas alınmıştır.

### 5.3 Önerilen modelin performans sonuçları

Önerilen modelin, sağlık ve yargı veri setleri üzerindeki test sonuçları Tablo 11'de gösterilmiştir. Önerilen model ile, Sağlık veri seti için %98,20 oranında, Yargı veri seti için ise %97,82 oranında erişim düzeyi sonuçlarının doğru tespit edildiği, ayrıca her iki veri seti için erişim hızı 0,85 ve 0,91 sn. olarak ölçüldüğü test edilmiştir.

Tablo 11. Erişim düzeyi ve erişim hızı sonuçları.

*Table 11. Access level and access speed results.*

| Kullanılan Veri Seti | Erişim Düzeyi (%) | Erişim Hızı |
|---|---|---|
| Sağlık Veri Seti | 98,20 | 0,85 sn. |
| Yargı Veri Seti | 97,82 | 0,91 sn. |

Önerilen modelin sunduğu sonuçlar değerlendirildiğinde, önerilen modelin iki farklı sektöre ait veri setinde %90 ve üzerinde doğru erişim düzeyi sunduğunu söyleyebiliriz. Ayrıca veri setindeki nesne sayısı arttıkça nesneye erişim hızının da arttığı gözlenmiştir.

### 5.4 Diğer erişim kontol modellerinin performans sonuçları

Rol Tabanlı Erişim Kontrolü, İsteğe Bağlı ve Zorunlu Erişim Kontrolü modellerinin, sağlık ve adalet veri setleri üzerindeki test sonuçları Tablo 12, Tablo 13 ve Tablo 14'te gösterilmiştir.

Tablo 12. Erişim düzeyi ve erişim hızı sonuçları (RBAC).

*Table 12. Access level and access speed results (RBAC).*

| Kullanılan Veri Seti | Erişim Düzeyi (%) | Erişim Hızı |
|---|---|---|
| Sağlık Veri Seti | 96,1 | 0,87 sn. |
| Yargı Veri Seti | 97,23 | 0,95 sn. |

Tablo 12. Erişim düzeyi ve erişim hızı sonuçları (DAC).

*Table 12. Access level and access speed results (DAC).*

| Kullanılan Veri Seti | Erişim Düzeyi (%) | Erişim Hızı |
|---|---|---|
| Sağlık Veri Seti | 90,88 | 0,87 sn. |
| Yargı Veri Seti | 90,52 | 0,92 sn. |

Tablo 13. Erişim düzeyi ve erişim hızı sonuçları (MAC).

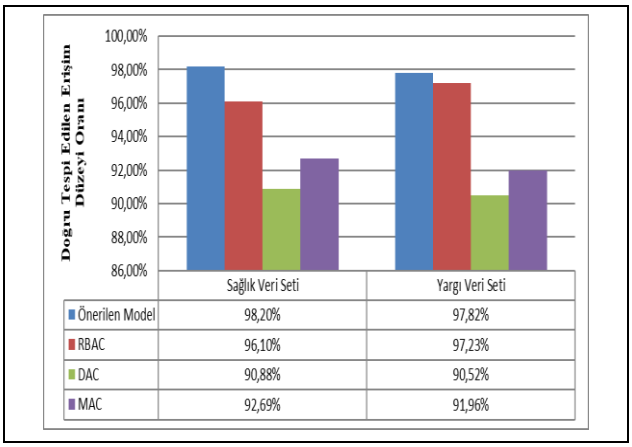
*Table 13. Access level and access speed results. (MAC).*

| Kullanılan Veri Seti | Erişim Düzeyi (%) | Erişim Hızı |
|---|---|---|
| Sağlık Veri Seti | 92,69 | 0,88 sn. |
| Yargı Veri Seti | 91,96 | 0,92 sn. |

Tablo 12, Tablo 13 ve Tablo 14'teki sonuçlar değerlendirildiğinde, her üç modelin iki farklı sektöre ait veri setinde %90 ve üzerinde doğru erişim düzeyi sunduğu, ancak bu oranların önerilen modelin altında seyrettiği tespit edilmiştir. Erişim hızının tüm modellerde yaklaşık benzer miktarlarda seyrettiği gözlenmişse de önerilen modelin diğer modellere kıyasla biraz daha verimli erişim hızı performansı gösterdiği test edilmiştir.

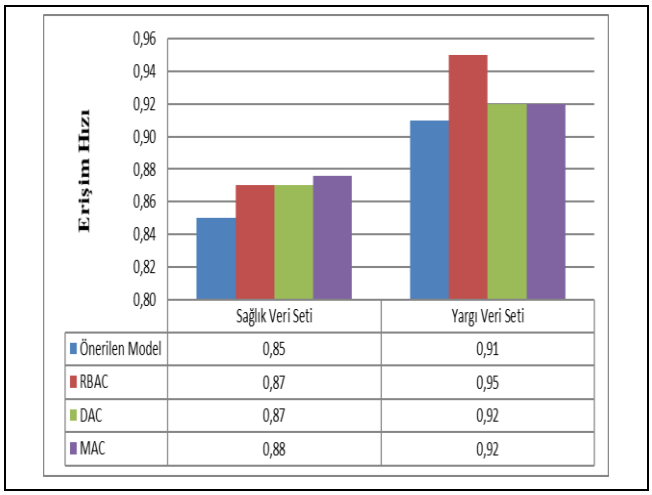
### 5.5 Performans değerlendirme

Önerdiğimiz modelin, diğer tekniklere oranla erişim düzeyi tespitinde ve erişim hızında daha başarılı sonuçlar verdiği, Şekil 15 ve Şekil 16'da görüleceği üzere özellikle her iki veri setinde de diğer modellere kıyasla daha yüksek oranlarda doğru erişim düzeyi tespit etme oranını yakaladığı ve erişim hızı performansının daha yüksek olduğu gözlemlenmiştir.




Şekil 15. Erişim düzeyi doğru tespit oranı.

*Figure 15. Access level accuracy detection rate.*




Şekil 16. Erişim hızı oranı

*Figure 16. Access speed rate.*

Sonuçları değerlendirdiğimizde, önerdiğimiz modelimizin diğer teknikler karşısında yetkilendirmede daha tutarlı ve bilginin paylaşımında daha hızlı sonuçlar veren bir teknik sunduğunu söyleyebiliriz.

## 6 Değerlendirme ve sonuç

Çalışmada ele aldığımız önerilen geliştirilmiş güvenlik modeli ile bilgi güvenliğinin temel unsurlarından olan bilginin *gizlilik* özelliğinin korunması ele alınmıştır. Modelin getirdiği güvenlik politikaları dağıtık veritabanı sistemlerine uygulanmış, böylece farklı fiziksel ortamlarda saklanan nesnelere kim tarafından ve nasıl erişilebileceği üzerine incelemeler yapılmıştır. Önerilen modelin sunduğu deneysel sonuçları değerlendirdiğimizde, önerilen modelimiz gerçek hayattan alınmış üç farklı sektöre ait veri setleri üzerine uygulanmış ve modelimizin performansı gerçek sistem uygulamalarında çok sık rastladığımız Rol Tabanlı Erişim Kontrolü (RBAC) ve Geleneksel Erişim Kontrolü (MAC/DAC) modelleri ile karşılaştırılmıştır. Önerdiğimiz modelin her üç veri setinde de %90 ve üzerinde doğru erişim izni ve erişim düzeyi sunduğu ve diğer modellere kıyasla her üç sektör için de ölçeklenebilir şekilde başarılı sonuçlar verdiği test edilmiştir. Çalışmanın artısı olarak, özellikle dağıtık sistem uygulamalarında sıklıkla karşılaşılan problemler ele alınmış, önerilen modelin dağıtık sistemlere genişletilebilir ve ölçeklenebilir olması ve yetkilendirmede daha tutarlı sonuçlar vermesi amaçlanmıştır.

Bu çalışmada önerdiğimiz model ile mevcut Bell-Lapuda modeli, yeni politikalar tanımlanarak geliştirilmiştir. Ayrıca bilgiyi yetki sahibi kullanıcıların kullanarak bilginin asıl sahiplerine hızlı bir şekilde iletilmesi sağlanmıştır. Bu modelle birlikte bilgi güvenliğinin üç temel unsuru gözetilerek mevcut modele esnek bir yapı kazandırılmıştır. Çalışmanın devamında, bilgi güvenliğinin temel unsurlarından olan erişilebilirlik ve bütünlük özellikleri de incelenecektir. İlaveten başka güvenlik modellerinin dağıtık veritabanı sistemlerine nasıl yayılacağı konusunda da araştırma yapılacaktır.

## 7 Conclusion

The proposed improved new access control model that we discussed in the study was implemented on a real distributed system. Thus, calculations were made on by whom and with which access permission and level the data stored in different physical environments could be accessed.

When we evaluated the experimental results provided by the proposed model, our proposed model was implemented on the data sets of two different sectors taken from real life, and the performance of our model was compared with the Role-based Access Control (RBAC), Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models that are encountered very often in real system applications. It was tested that the proposed model provided a more accurate access level and access rate in both data sets compared to other models. As a plus of the study, the restrictions in the use of resources, which are frequently encountered in distributed system applications, were minimized with the special rights and powers and controls created, and it was observed that the proposed model could be expanded for different sector data.

With the model we propose in this study, the existing Bell-Lapuda model was developed by defining new policies. In addition, it was ensured that the information is quickly transmitted to the original owners by using the authorized users. With this model, a flexible structure has been given to the existing model by considering the three basic elements of information security.

In the continuation of the study, our proposed model will be developed, and a new framework based on the access location and user behaviors in its design will be presented.

## 8 Yazar katkı beyanı

Gerçekleştirilen çalışmada Çiğdem BAKIR ve Mehmet GÜÇLÜ fikrin oluşması, tasarımın yapılması, literatür taraması, analizlerin gerçekleştirilmesi, sonuçların incelenmesi, yazım denetimi ve içerik açısından makalenin kontrol edilmesi kısımlarında ortak katkıda bulunmuştur.

## 9 Etik kurul onayı ve çıkar çatışması beyanı

Hazırlanan makalede etik kurul izni alınmasına gerek yoktur. Hazırlanan makalede herhangi bir kişi/kurum ile çıkar çatışması bulunmamaktadır.

## 10 Kaynaklar

[1] Andress J. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice Algorithms*. 2nd ed. USA, Elsevier, 2011.

[2] Sukumarana SC, Misbahuddinb M. "PCR and bio-signature for data confidentiality and integrity in mobile cloud computing". *Journal of King Saud University-Computer and Information Sciences*, 33(4), 426-435, 2021.

[3] Whitman M, Mattord HJ. *Principles of Information Security.* 4th Course Technology, USA, Cengage Learning, 2012.

[4] Ferraiolo DF, Kuhn, DR. "Role based access control". *15th National Computer Security Conference,* Gaithersburg, USA, 13-16 October 1992.

[5] Abidin S, Rana V. "On confidentiality, integrity, authenticity and freshness (CIAF) in WSN". *Advances in Computer Communication and Computational Sciences*, 1158(1), 87-97, 2021.

[6] Charaf L, Allihamidi I, Addaim A. "A distributed XACML based access control architecture for IoT systems". *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET),* Meknes, Morocco, 16-19 April 2020.

[7] Shin MS, Jeon HS, Ju YW, Lee BJ, Jeong, SP. "Constructing RBAC based security model in u-healthcare service platform". *The Scientific World Journal*, 2015(4), 1-13, 2015.

[8] Ge C, Liu Z, Fang L. "A blockchain based decentralized data security mechanism for the Internet of things". *Journal of Parallel and Distributed Computing,* 141, 1-9, 2020.

[9] Chow SM, Lee JH, Subramanian, L. "Two-party computation model for privacy-preserving queries over distributed databases". *Network and IT Security Conference, NDSS Symposium*, California, USA, 08-11 February 2009.

[10] Kumar R, Bhatia MP. "A Systematic review of the security in cloud computing: Data integrity, confidentiality and availability". *2020 IEEE International Conference on Computing Power and Communication Technologies (GUCON),* Greater Noida, India, 2-4 October 2020.

[11] Kotari M, Chiplunkar NN. "Investigation of security issues in distributed system monitoring". *Information Sciences, Springer*, 2020. http://doi: 10.1007/978-3-030-22277-2_24.

[12] Kotari M, Chiplunkar NN, Nagesh HR. "Framework of security mechanisms for monitoring adaptive distributed systems". *IOSR Journal of Computer Engineering (IOSR-JCE)*, 18(4), 25-36, 2016.

[13] Naeem W, Shah MA, Malik AK. "Privacy-preserving in collaborative working environments". *Proceedings of the IOARP International Conference on Communication and Networks*, London, United Kingdom, 1-3 December 2015.

[14] Bertolissi C, Fernandez, M. "A metamodel of access control for distributed environments: Applications and properties". *Information and Computation*, 238, 187-207, 2014.

[15] Bertolissi C, Fernandez, M. "A metamodel of access control for distributed environments: Applications and properties". *Information and Computation Journal*, 238(1), 187-207, 2014.

[16] Dasgupta D, Roy A, Ghosh D. "Multi-user permission strategy to access sensitive information". *Information Sciences, Elsevier,* 2017. http://doi: 10.1016/j.ins.2017.09.039.

[17] Balamurugan B, Shivitha NG, Monisha V, Saranya, V. "A Honey bee behaviour inspired novel attribute-based access control using enhanced bell-lapadula model in cloud computing". *Innovation Information in Computing Technologies (ICIICT), 2015 International Conference on,* IEEE, Chennai, India, 19-20 Februrary 2015.

[18] Özsu MT, Valduriez P. *Principles of Distributed Database Systems.* 3rd ed. USA, Springer Science & Business Media, 2011.

[19] Rahimi SK, Haug FS. *Distributed Database Management Systems: A Practical Approach*. 3rd ed. New York, USA, Wiley India Private Limited, 2015.

[20] Tchernykh A, Schwiegelsohn U, Babenko M. "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability". *Journal of Computational Science*, 36, 1-9, 2019.

[21] Elmagarmid A, Rusinkiewics M, Sheth A. *Management of Heterogeneous and Autonomous Database Systems*. 1st ed. San Francisco, California, Morgan Kaufmann Publishers, 1999.

[22] Zhang Y, Ye X, Xie F, Peng Y. "A practical database intrusion detection system framework". *2009 Ninth IEEE International Conference on Computer and Information Technology*, Xiamen, China, 11-14 October 2009.

[23] Kumar R, Tripathi R. "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell-LaPadula model". *Journal of Ambient Intelligence and Humanized Computing*, 12(1) 2321-2338, 2021.

[24] Crampton J, Leung W, Beznosov K. "The secondary and approximate authorization model and its application to Bell-LaPadula policies". *ACM Symposium on Access Control Models and Technologies,* California, USA, 07 June 2006.

[25] Sánchez R, Steven AD, Mohammed SB. "A service-based RBAC & MAC approach incorporated into the FHIR standard". *Digital Communications and Networks*, 5(4), 214-225, 2019.

[26] Pitts A. "Foundations of software science and computation structures". FoSSaCS: *International 18th International Conference on Theory and Practice of Software*, London, UK, 11-18 April 2005.

[27] Thuraisingham B. "Security for distributed databases". *Information Security Technical Report,* 6(2), 95-11, 2001.

[28] Bertino E, Sandhu R. "Database security-concepts, approaches and challenges". *IEEE Transactions on Dependable and Secure Computing,* 2(1), 2-19, 2005.

[29] Özcanhan MH. "A new peculiarity to intelligent doors: Security through information sharing". *Pamukkale University Journal of Engineering Sciences,* 23(5), 581-587, 2017.

[30] Gunduz MZ, Daş R. "Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları". *Pamukkale Mühendislik Fakültesi Dergisi,* 24(2), 327-335, 2018.