Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi

Afyon Kocatepe University Journal of Science and Engineering

AKÜ FEMÜBİD **22** (2022) 015103 (126-135) AKU J. Sci. Eng. **22** (2022) 015103 (126-135)

DOI: 10.35414/akufemubid.932490

Araştırma Makalesi / Research Article

Dağıtık Veritabanları için Geliştirilmiş Yeni Güvenlik Modeli

Çiğdem BAKIR[1*], Mehmet GÜÇLÜ[2]

[1] *Kütahya Dumlupınar Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü, Kütahya, Türkiye.*

[2] *Yıldız Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye.*

Sorumlu Yazar e-posta: cigdem.bakr@gmail.com. *ORCID ID: http:// orcid.org/0000-0001-8482-2412*

mehmetguclu007@ gmail.com *ORCID ID: https://orcid.org/0000-0002-7507-5694*

Geliş Tarihi: 04.05.2021 Kabul Tarihi: 15.02.2022

Öz

Erişim denetimleri, günümüz bilgi sistemlerini güven altına almak için geliştirilmiş önemli bir araçtır. Kurumlar erişim denetimlerini özellikle çalışanlarının kim olduğunu, çalışanlarının neler yapabileceklerini, hangi kaynaklara erişebileceklerini ve hangi işlemleri gerçekleştirebileceklerini tanımlamak ve tüm bu süreci yönetmek için kullanırlar. Dağıtık veritabanı sistemlerine sahip kurumlar için ise bu süreç oldukça maliyetli bir iştir. Nitekim farklı sunucular üzerinde dağıtılan ve biri diğerine mantıksal olarak bağlı olan kaynaklara ulaşmak isteyen kullanıcıların tanımlanması, istekte bulunan kullanıcının doğrulanması ve yetkilendirilmesi her zaman etkin bir şekilde yapılandırılamadığından erişim denetimleri yeterince nitelikli bir biçimde gerçekleştirilememektedir. Çalışmamızda önerilen model ile, dağıtık veritabanı sistemlerinde tanımlı tüm kullanıcıların nesneler üzerindeki izin ve erişim düzeylerinin otomatik olarak hesaplanması, böylece kullanıcıların hangi nesneye erişim yapabileceklerine daha etkin bir şekilde karar verilmesi ve ihtiyaç duymadıkları bilgiye erişim yapmalarının ise engellenmesi amaçlanmıştır. Çalışmada önerilen geliştirilmiş model, gerçek hayattan alınmış veri kümesi üzerine uygulanmıştır. Önerilen modelin performansı, Geleneksel Erişim Denetimi modellerinin performansları ile karşılaştırılmıştır. Elde edilen sonuçlar kıyaslandığında, önerilen modelin birçok dağıtık veritabanı sistemlerine ölçeklenebilir olmasının yanında daha doğru erişim düzeyi sonuçlarını veren bir erişim kontrol modeli sunduğu test edilmiştir.

Anahtar kelimeler
Erişim Denetimi;
Dağıtık Veritabanı;
İzin Düzeyi;
Erişim Düzeyi

New Security Model Developed for Distributed Databases

Abstract

Access controls are an important tool developed to secure today's information systems. Organizations especially use access controls to define who their employees are, what their employees can do, which resources they can access and which operations they can perform, and to manage the entire process. For organizations with distributed database systems, this process is a costly task. As a matter of fact, since the conditions for identifying users who want to access resources distributed on different servers and logically connected to one another, authentication and authorization of the requesting user and monitoring the actions of the user cannot always be effectively configured. With the proposed model in our study, it is aimed to automatically calculate the permission and access levels of all users defined in distributed database systems, so that users can decide which object they can access more effectively and prevent them from accessing the information they do not need. The developed model proposed in the study was applied on a real-life data set. The performance of the proposed model has been compared with the performances of Traditional Access Control models. When the obtained results are compared, it has been tested that the proposed model offers an access control model that provides more accurate access level results besides being scalable to many distributed database systems.

Keywords
Access Control;
Distributed Database;
Permission Level;
Access Level

1. Giriş

Günümüzde bilgi sistemlerine ve kaynaklarına zarar veren yeni tehditler vardır: zırhlı virüsler (armored virus), fidye yazılımları (ransomware) ve kötücül kripto – kilitleyici yazılımlar (cryptolocker malware) (Whitman and Mattord 2012). Sistemleri bu zararlı tehditlere karşı korumak için atılan en girişken adımlara rağmen saldırganların bazen başarılı olabildikleri görülmektedir. Bilgi güvenliğinin üç temel unsurlarından olan gizlilik, bütünlük ve erişebilirlik prensiplerinden herhangi birinin ihlaline neden olan her olay bir güvenlik ihlalidir (Solomon and Kim 2016). Bazı ihlaller kasten sistemleri erişilemez kılar ve hizmetleri sekteye uğratırken, bazıları ise kazaen yazılım veya donanım arızaları nedeniyle oluşur. Güvenlik ihlalleri ister kaza sonucu ister kötücül olsun bir kurumun faaliyetini ve güvenirliliğini ciddi bir şekilde etkiler.

Güvenlik ihlallerine neden olan faktörlerin başında hizmet reddi (Denial of Service – DOS) saldırısı, dağıtık hizmet reddi (distributed Denial of Service - DDOS) saldırısı, webte uygunsuz gezinme davranışları, izinsiz dinleme (Wiretapping), arka kapı (backdoor) kullanarak kaynaklara erişim ve kaza sonucu veya kasten oluşan veri değişiklikleri gelmektedir (Whitman and Mattord 2012). Kasten veya kazaen değiştirilen veriler, bilişim sistemleri güvenliğinin bütünlük ilkesini etkiler ve bir güvenlik ihlalinin doğmasına sebebiyet verir. Kasten veya kazaen veri değiştirme olaylarının ortaya çıkmasında özellikle kullanıcılara gereğinden fazla yetki verilmesi ve yetkilerin denetiminin zayıf tutulması önemli bir rol oynar (Andress, 2011). Bu tür sorunlar ile başa çıkmak için organizasyonların boyutuna ve kullanıcılar için gereken özel erişim haklarına göre tasarlanmış iyi bir erişim denetimi modeline ihtiyaç vardır.

Günümüzde birçok uygulama alanına özgü tasarlanmış erişim kontrol modelleri mevcuttur. Ancak bu modellerin, sayısı hızla artan ve gittikçe daha karmaşık hale gelen sistemler üzerinde ihtiyaçları tam olarak karşılayamadığını, sistemlere ciddi bir mali yük getirdiğini, bilgi akış denetimini tam olarak sağlayamadığını ve uygulamada esnekliğin çok büyük bir oranda yitirilmesine sebebiyet verdiğini görmekteyiz (Kotari and Chiplunkar 2020, Kotari *et al.*2016, Shin *et al.* 2015, Reid *et al.* 2014). Bu nedenle erişim kontrol modellerinin, bilgi sistemlerini sadece yetkisiz erişimlerden, kötü niyetli kullanıcılardan ve hatalı kullanımlardan koruyacak şekilde yapılandırılmış olmasının tek başına yeterli olmadığı, aynı zamanda kolay yönetilebilir ve ölçeklenebilir olması, organizasyon yapısına uygun ve erişim kontrolü işlevselliğinin tutarlı bir şekilde tasarlanmış olmasının da büyük önem taşıdığı gözlenmektedir.

Çalışmamızda, uygulamalarda sıklıkla karşılaşılan problemler ele alınarak, daha işlevsel, kolay yönetilebilir ve ölçeklenebilir, yetkilendirmede daha tutarlı sonuçlar verebilen bir erişim kontrol modeli geliştirilmiştir. Çalışmanın asıl katkısı, önerilen model ile dağıtık veritabanı sistemlerinde aktif rol alan tüm kullanıcıların nesneler üzerindeki izin ve erişim düzeylerinin otomatik olarak hesaplanması, gereğinden fazla yetkilendirmeden kaçınılarak kullanıcıların hangi nesneye erişim yapabileceklerine daha etkin bir şekilde karar verilmesi ve ihtiyaç duymadıkları bilgiye erişim yapmalarının ise engellenmesi amaçlanmıştır.

Bu çalışmanın geri kalan kısmı şu şekilde organize edilmiştir: 2. ilgili çalışmalar, 3. bölümde materyal ve yöntem, 4. Önerilen method, 5. bölümde deneysel çalışma ve 6. bölümde sonuç yer alacaktır.

1.1 İlgili Çalışmalar

Günümüzde bulut bilişim, Bilgi Teknolojisi (BT) sektörünün gelişmiş alanlarından biridir. İnternette birçok bilgisayar korsanı ve kötü niyetli kullanıcı bulunduğundan, bulut ortamında verilerin gizliliğini sağlamak oldukça önemlidir. Bu amaçla son zamanlarda bulut bilişim odaklı geliştirilmiş erişim kontrol modellerinin sayısının hızla arttığı görülmektedir (Li *et al.*2016, Lu *et al.*2016). Yeni güvene dayalı bir erişim kontrol metodu geliştirilmiştir (Behera and Khilar 2016). Önerilen model, kullanıcıyı bulut ortamına girmeden önce kullanıcı güven değerine göre yetkilendirir. Bunun için de hem kullanıcı hem de bulut kaynaklarının güven değeri hesaplanır. Hem kullanıcıların hem de bulut kaynaklarının güven değeri eşik değerlerinden yüksekse, güvenilir olarak kabul edilir. Bulut bilişim için geçerli kılınan mevcut erişim kontrol modelleri

ve hizmetlerini açıklayan başka bir çalışmada ise, bulut bilişimin güvenliğini artıran ve yetkisiz kullanıcının bulut kaynaklarına erişimini engelleyen bir erişim kontrol modeli sunulmuştur (Pandey *et.al* 2016).

Mevcut Dağıtık Kontrol Sistemi (DKS) ortamlarında, erişim kontrol ilkeleri birçok heterojen sistem arasında dağıtıldığı için en az ayrıcalık ilkesine uymak zordur. Bazı çalışmalarda, dağıtık sistemlerde daha eksiksiz ve yönetilebilir bir erişim kontrol modeline doğru ilerlemelerde yaşanan temel zorluklardan bahsedilmiştir [Kotari *et al.*2016, 7 Reid *et al.* 2014, Huh 2016). Bir çalışmada, her erişimin en az ayrıcalık ilkesine uyan politikalara karşı kontrol edilmesi için Endüstriyel Kontrol Sistemi (EKS) topluluğu tarafından uyarlanabilecek bir erişim kontrol mimarisi sunulmuştur (Huh 2016). Önerilen mimaride merkezi politika yönetiminin ve bağlı her saha cihazının korunması amaçlanmıştır. Dağıtık ortamların özel gereksinimlerini dikkate alan tasarlanmış erişim kontrolü için bir metamodel tanımlanmıştır(Bertolissi and Fernandez 2014). Çalışmada, her biri kendi kaynaklarını koruyacak şekilde birkaç siteden oluşan bir dağıtık sistem üzerinde, her bir üye tarafından belirlenen yerel politikaları göz önüne alan erişim kontrol politikalarının uygulanması için bir çerçeve önerilmiştir.

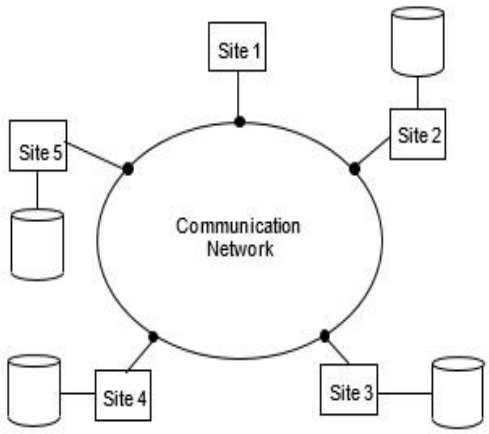
Veri erişimi, rol tabanlı veya politika tabanlı erişim denetimleri kullanılarak statik bir şekilde denetlenebilir. Ancak günümüzün devasa ve yapılandırılmamış verilerini depolamak için çok fazla araştırma çalışmasının yapıldığı büyük veri çağında, veri erişim güvenliğini sağlama konusunda hala büyük bir boşluk olduğu görülmektedir (Szczypiorski *et al.* 2018, Angin and Ranchal 2019). Havaalanı arama / gözetleme, savunma ve hastane yönetim sistemleri gibi statik erişim kontrol sistemlerinin etkili olmadığı birçok gerçek dünya uygulaması vardır (Srivastava and Shekokar 2020, Thuraisingham 1997.). İstekte bulunanın gerçekliğine göre öğrenen ve adapte olan bir sisteme ihtiyaç vardır. Mevcut rol tabanlı erişim kontrol yöntemi davetsiz misafirleri kolayca çeker. Yine politikaya dayalı erişim kontrolünde ise, başlangıçta karar verilen politika dinamik olarak değiştirilemediğinden uyum eksikliği ortaya çıkar. Srivastava and Shekokar tarafından önerilen risk uyarlamalı erişim kontrolü, talep sahibinin gerçekliğini anlayan, riski hesaplayan ve daha sonra buna göre hareket eden bir çerçeve sunar. Bu çerçeve, tasarımında erişim süresi, erişim yeri, talep sahibinin önceki geçmişi (aynı talebin kaç kez tekrarlandığı) ve talep edilen bilgilerin hassasiyeti gibi birçok gerçek dünya niteliğini göz önünde bulundurur. Bu çalışma amaç ve kapsam olarak bizim çalışmamız ile benzerlik gösterse de, bizim çalışmamızda kullanıcının geçmiş eylemlerine veya erişim taleplerine bakılmaz. Çalışmamızda önerdiğimiz model, her kullanıcıya organizasyon yapısına uygun farklı boyutlarda bir değer atar ve nesneye erişim iznini, kullanıcının boyut değerleri ve erişim düzeyleri ile ilişkilendirir. Yani bir kullanıcının sahip olduğu yeteneklere veya değerlere göre o kullanıcının bir nesne üzerindeki erişim iznini ve düzeyini hesaplar.

2. Materyal ve Metot

Bu bölümde, deneysel çalışmalarda kullandığımız Dağıtık Veritabanı Sistemi, Rol Tabanlı Erişim Kontrol Modeli ve Geleneksel Erişim Kontrol Modeli hakkında kısaca bilgi verilecektir.

2.1 Dağıtık Veritabanı Sistemi

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 (Özsu and Valduriez 2011).

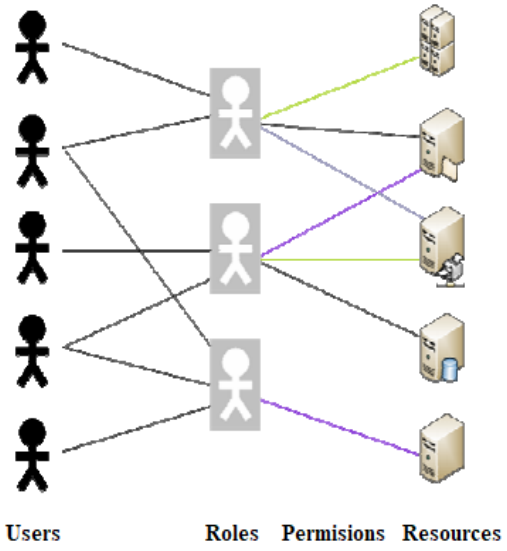


Şekil 1. Dağıtık veritabanı barındıran sunucular

Şekil 1'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.

2.2 Rol Tabanlı Erişim Kontrol Modeli (RBAC)

Kullanıcıların bir organizasyon içerisindeki görev ve sorumluluklarına göre roller tanımlanır ve kaynaklara erişim yetkisi ve sınırı bu rollere göre şekillendirilir (Solomon and Kim 2016). 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.

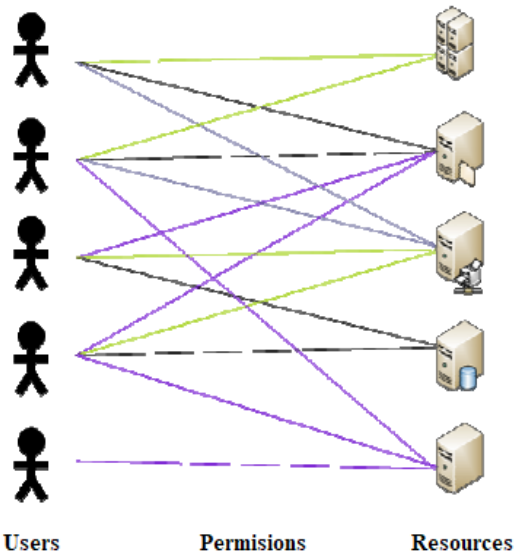


Şekil 2. Rol Yapısı

Şekil 2'de kullanıcılar, roller ve yetkiler arasındaki ilişki gösterilmektedir. Yetkiler, nesneler (sistemler, sunucular, dosyalar, uygulamalar, vs.) üzerinde yapılabilecek işlemlerdir ve rollere tanımlanırlar. Kullanıcılara roller atanarak birtakım yetkilere sahip olmaları sağlanır. Her rol için bir veya daha fazla kaynağa erişim yetkisi verilir ve her kullanıcıya bir ya da daha fazla rol atanır [2].

2.3 Geleneksel Erişim Kontrol Modeli (MAC/DAC)

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 (Solomon and Kim 2016). 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 (Elmagarmid and Sheth 1999).



Şekil 3. Geleneksel Yetkilendirme

Şekil 3'te kullanıcılar ve yetkiler arasındaki ilişki gösterilmektedir. Yetkiler, nesneler (sistemler, sunucular, dosyalar, uygulamalar, vs.) üzerinde yapılabilecek işlemlerdir. Kullanıcılar, kendilerine atanmış yetkilere göre kaynaklara erişim sağlar.

3. Önerilen Method

Veriler nesne olarak ifade edilir. Kullanıcılar ise güvenlik boyutlarına göre sınıflandırılır. Bir güvenlik boyutu, bir kullanıcının özelliklerini açıklar ve her boyut kullanıcılara atanabilen birkaç değer içerir. Örneğin Tablo 1'de kullanıcıların Birim, Güvenlik Sınıflandırması, İş Unvanı ve Operasyon şeklinde

isimlendirilen farklı güvenlik boyutlarında sahip olabileceği birkaç değer gösterilmiştir. Bir kullanıcıya atanabilecek Güvenlik Boyutlarından Birim boyutu "Birim A, Birim B, Birim C, Birim D ve Birim E", Güvenlik Sınıflandırması boyutu "Çok Gizli, Gizli, Özel ve Kısıtlı", İş Unvanı boyutu "Başhekim, Doktor, BT Personeli, Hemşire, Satın Alma Personeli" ve Operasyon boyutu "İşlem A, İşlem B, İşlem C, İşlem D, İşlem E ve İşlem F" değerlerinden oluşur.

Çizelge 1. Güvenlik Boyutları

Güvenlik Boyutu	Güvenlik Boyutu	Güvenlik Boyutu	Güvenlik Boyutu
Ad: Birim	**Ad: Güvenlik Sınıflandırması**	**Ad: İş Unvanı**	**Ad: Operasyon**
Birim A	Çok Gizli	Başhekim	İşlem A
Birim B	Gizli	Doktor	İşlem B
Birim C	Özel	BT Personeli	İşlem C
Birim D	Kısıtlı	Hemşire	İşlem D
Birim E		Satın Alma Personeli	İşlem E
			İşlem F

Bir güvenlik boyutu şu özelliklere sahip olabilir:

Sıralı:
Bir boyut sıralı ise, boyut değerleri sıralanmış ve sıra düzenseldir ve bir kullanıcıya atanan değer altındaki değerleri de kapsar. Örneğin, Güvenlik Sınıflandırması adlı boyutta Çok Gizli, Gizli, Özel ve Kısıtlı değerleri bulunur. Gizli değeri atanmış bir kullanıcı, otomatik olarak Özel ve Kısıtlı değerlerini de taşımaktadır.

Sırasız:
Bir boyut sırasız ise, boyut değerleri sıralanmış değildir ve bir kullanıcıya birden çok değer atanabilir. Örneğin, Operasyon adlı boyutta İşlem A, İşlem B, İşlem C, İşlem D, İşlem E ve İşlem F değerleri bulunur. Bir kullanıcı, hem İşlem C hem de İşlem E operasyon içinde yer alabilir.
İş unvanı Başhekim olan bir kullanıcı, diğer kullanıcılara boyut değerlerini atar. Her kullanıcıya her boyuttan en az bir değer atanmış olmalıdır. Ancak bazı boyutlarda birkaç değer atanabilir. Örneğin, Tablo 2'de beş kullanıcıdan her biri farklı birimlerde yer almakta, E biriminde bulunan ve C ve D işlemlerini yapabilen Kullanıcı1, özel güvenlik sınıfından bir hemşire iken, A biriminde bulunan ve A, B ve F işlemlerini yapabilen Kullanıcı4, Gizli güvenlik sınıfından bir Doktor'dur.
Her bir kullanıcı, erişim denetimi için boyut değerlerini kullanır. Her kullanıcı, bir nesneye erişebileceği zaman boyut değerlerine göre erişim yapar ya da yapamaz. Yani bir kullanıcı, tüm güvenlik boyutlarından aldığı değerlere göre bir nesne üzerinde okuma ve yazma erişimine sahip olabilir. Erişim izin listesi, her erişim boyutundan bir değer içermelidir. Bununla beraber, aynı boyuttan birkaç değeri de içerebilir (İşlem A, İşlem B ve İşlem F gibi). Her güvenlik boyutundan alınan boyut değerine göre kullanıcıların nesne üzerindeki erişim düzeyi belirlenir. Örneğin İş Unvanı güvenlik boyutunda yer alan Satın Alma Personeli için okuma ve yazma erişim düzeyi ve Hemşire için yalnızca okuma erişim düzeyi belirlenebilir.

Çizelge 2. Beş Farklı Kullanıcıya Ait Boyut Değerleri

Güvenlik Boyutu	Kullanıcı1	Kullanıcı2	Kullanıcı3	Kullanıcı4	Kullanıcı5
Birim	Birim E	Birim B	Birim D	Birim A	Birim C
Güvenlik Sınıflandırması	Özel	Gizli	Özel	Gizli	Çok Gizli
İş Unvanı	Hemşire	Satın Alma Personeli	Hemşire	Doktor	BT Personeli
Operasyon	İşlem C, D	İşlem B, E, F	İşlem C, D, E	İşlem A, B, F	İşlem A, B, C, D, E, F

3.1. İzin Düzeyleri

İzin düzeyleri, bir nesnenin güvenlik ayarlarını değiştirebilmek için farklı yetenek düzeyleridir. Bir nesnedeki izin düzeyi, nesnenin izinleriyle toplu olarak belirlenir. Eğer izin düzeyi,

İzin verildi ise; Nesnenin güvenlik ayarları değiştirilebilir.

Yok ise; Nesnenin güvenlik ayarları değiştirilemez olarak yorumlanır.

Bir nesnenin izin düzeyi "İzin verildi" ise nesne aranabilir ve güvenlik ayarları değiştirilebilinir, ancak erişim düzeyi "Yok" ise nesne görüntülenemez.

3.2. Erişim Düzeyleri

Erişim düzeyleri, bir nesneyi görme ya da değiştirmeye yönelik farklı yetenek düzeyleridir. Bir nesneye erişim düzeyi, nesnedeki erişim izinleriyle toplu olarak belirlenir.

i. Bir kullanıcının erişim düzeyi ***Okuma/Yazma*** ise**;** Nesne görüntülenebilir ve değiştirilebilinir.

ii. Bir kullanıcının erişim düzeyi ***Yalnızca Okuma*** ise**;** Nesne görüntülenebilir, ancak değiştirilemez.

iii. Bir kullanıcının erişim düzeyi ***Örtülü*** ise**;** Nesnenin var olduğu görülebilir, ancak özellikleri görüntülenemez.

iv. Bir kullanıcının erişim düzeyi ***Yok*** ise**;** Nesne görüntülenemez. Nesne, arama sonuçlarında yoktur.

3.3. Erişim ve İzin Düzeylerini Hesaplama

Bir nesneye erişim izni, boyut değerleri (kullanıcının her bir boyutta almış olduğu değerdir, örneğin Tablo 2'de 5 farklı kullanıcıya tanımlanmış değerler gibi) ve erişim düzeyi (Okuma/Yazma, Yalnızca Okuma, Örtülü veya Yok) ile ilişkilendirilir. Yani bir kullanıcının sahip olduğu yeteneklere veya boyut değerlerine göre o kullanıcının bir nesne üzerindeki erişim izni ve düzeyi ortaya çıkarılır. Eğer kullanıcının erişim düzeyi örtülü veya üzeri ise (Örtülü, Yalnızca Okuma, Yalnızca Yazma, Okuma / Yazma) o kullanıcının nesneye erişimine izin verilir.

3.3.1. Bir Boyuttaki Erişim Düzeyi ya da İzin Düzeyini Hesaplama

Bir nesne üzerindeki erişim izinleri, bir boyut içindeki değerleri birden çok erişim düzeyiyle ilişkilendirebilir (Örneğin bir kullanıcı Operasyon boyutunda yer alan "İşlem B" değeri için yalnızca okuma erişim düzeyini alabilirken, "İşlem C" değeri için ise okuma ve yazma erişim düzeylerini birlikte alabilir). Benzer durum izin düzeyleri için de geçerli olabilir. Bu durumlarda en az kısıtlayıcı erişim ve izin düzeyleri kullanılır.

Bir örnek üzerinden bu durumu anlatacak olursak; bir kullanıcıya aşağıdaki boyut değerleri atanmış olabilir (Tablo 3).

Çizelge 3. Kullanıcı1'e Tanımlanmış Boyut Değerleri

Güvenlik Boyutu	Kullanıcı1
Birim	Birim E
Güvenlik Sınıflandırması	Özel
İş Unvanı	Hemşire
Operasyon	İşlem C, D

Kullanıcı, şu erişim izinlerine sahip nesneyi görüntüleyebilir (Tablo 4):

Çizelge 4. Bir Nesneye Ait Erişim Düzeyleri

Güvenlik Boyutu	Boyut Değeri	Erişim Düzeyi
Birim	Birim E	Yalnızca Okuma
Güvenlik Sınıflandırması	Gizli	Yalnızca Yazma
Güvenlik Sınıflandırması	Özel	Yalnızca Okuma
Güvenlik Sınıflandırması	Özel	Örtülü
Operasyon	İşlem A	Okuma
Operasyon	İşlem D	Okuma / Yazma

Nesne şu izinlere sahip olabilir (Tablo 5):

Çizelge 5. Nesnenin Erişim İzinleri

Güvenlik Boyutu	Boyut Değeri	İzin Düzeyi
İş Unvanı	*Doktor*	İzin verildi

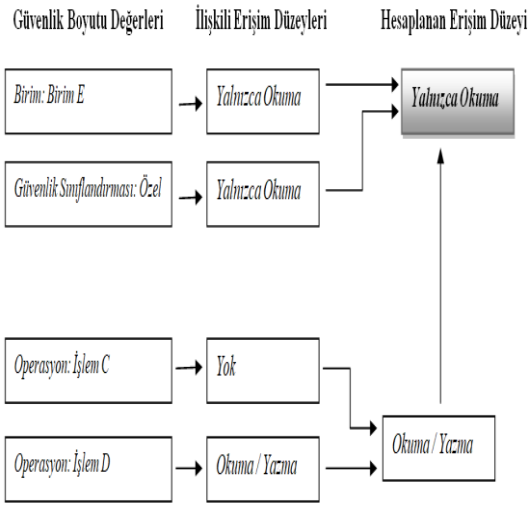
Nesne erişim izinleri, Operasyon boyutundaki İşlem D kullanıcı üyeliğinin *Okuma/Yazma* erişimiyle sonuçlandığını belirtir. Operasyon boyutundaki İşlem A için tanımlanmış bir erişim izni olmadığından, Operasyon boyutundaki İşlem A için kullanıcı üyeliği "Yok" erişim düzeyiyle sonuçlanır. Bu erişim düzeylerinden en az kısıtlayıcı olan Okuma ve Yazma düzeyidir; bu nedenle, Operasyon boyutu için bu erişim düzeyi kullanılır.

Nesne erişimi izinleri, kullanıcının Özel Güvenlik Sınıflandırmasının en az kısıtlayıcı olan *Yalnızca Okuma* erişimiyle sonuçlandığını belirtir. Nesne, Hemşire Unvanını bir izin düzeyiyle ilişkilendirmek için herhangi bir izne sahip olmadığından, sonuç "Yok" izin düzeyidir.

3.3.2. Nesne Üzerindeki Genel Erişim ya da İzin Düzeyini Hesaplama

Her boyutta en az kısıtlayıcı erişim ya da izin düzeyinin hesaplanması, her boyut için farklı düzeylerle sonuçlanabilir. Bu durumda her boyutta en az kısıtlayıcı erişim ya da izin düzeyi kullanılır.

Genel hesaplama Şekil 6'da gösterilmiştir. Şekil 4'e göre Birim boyutu için *Yalnızca Okuma* erişim düzeyi, Operasyon boyutu için *Okuma* ve *Yazma* erişim düzeyi, Güvenlik Sınıflandırması boyutu için ise *Yalnızca Okuma* erişim düzeyi kullanılır. Bu düzeylerin en kısıtlayıcısı *Yalnızca Okuma* olduğundan, kullanıcının nesnede aldığı genel erişim düzeyi ***Yalnızca Okuma*** olur.



Şekil 4. Erişim Düzeyi Hesaplama

4. Deneysel Çalışma

Çalışmada sağlık, eğitim ve kamu hizmeti veren işletmelerden alınan üç farklı gerçek veri seti kullanılmış, önerilen erişim kontrol modeli ve diğer yöntemlerin başarısı her bir veri setinde elde edilen sonuçlara göre değerlendirilmiştir.

4.1. Veri Kümeleri

Çalışmada kullanılan farklı sektörlerden alınmış üç 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 107 kullanıcı, 36.251 nesne ve 8 güvenlik boyutundan, Eğitim sektöründen alınan veri kümesi 292 kullanıcı, 72.988 nesne ve 6 güvenlik boyutundan ve Kamu sektöründen alınan veri kümesi 1.355 kullanıcı, 752.220 nesne ve 11 güvenlik boyutundan oluşmaktadır. Veri setleri "Sağlık Veri Seti", "Eğitim Veri Seti" ve "Kamu Veri Seti" olarak ifade edilmiştir.

4.2. Deneysel Analizler

Önerilen modelimiz ile birlikte diğer erişim kontrol modelleri de gerçek bir dağıtık sistem sunan platform üzerinde çalıştırılmış ve tüm modeller üç veri setine ayrı ayrı uygulanmıştır. Her bir veri setine uygulanan tüm modeller için elde edilen izin ve erişim düzeyi sonuçları, veri setinin alındığı sektöre ait uygulamada geçen izin ve erişim düzeyi sonuçları ile karşılaştırılarak metotların performans değerleri analiz edilmiştir. Veri kümelerine uygulanan metotların performans değerlendirilmesinde her metodun doğru izin ve erişim düzeyi tespit yüzdeleri esas alınmıştır.

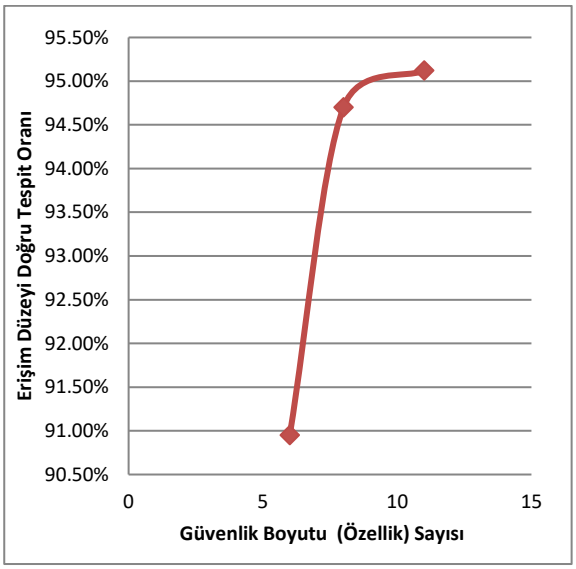
4.2.1. Önerilen Modelin Performans Sonuçları

Önerilen modelin, sağlık, eğitim ve kamu veri setleri üzerindeki test sonuçları Tablo 6'da gösterilmiştir. Önerilen model ile, Sağlık veri seti için %98,20 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %94,70'inde erişim düzeylerinin doğru tespit edildiği, Eğitim veri seti için %95,03 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %90,95'inde erişim düzeylerinin doğru tespit edildiği ve Kamu veri seti için %97,91 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %95,12'sinde erişim düzeylerinin doğru tespit edildiği test edilmiştir.

Çizelge 6. Önerilen Modelin İzin ve Erişim Düzeyi Performansı

	Erişim İzni	Erişim Düzeyi
Sağlık Veri Seti	98,20%	94,70%
Eğitim Veri Seti	95,03%	90,95%
Kamu Veri Seti	97,91%	95,12%

Önerilen modelin sunduğu sonuçlar değerlendirildiğinde, önerilen modelin üç farklı sektöre ait veri setinde %90 ve üzerinde doğru erişim izni ve erişim düzeyi sunduğunu söyleyebiliriz. Ayrıca güvenlik boyutu (özellik sayısı) arttıkça erişim düzeyinde tespit edilen başarı oranının da arttığı (Şekil 5), nitekim kullanıcı ve nesne sayısı diğer veri setlerine kıyasla daha fazla olan Kamu veri setinde başarı oranının daha yüksek çıkmasında güvenlik boyutu sayısının diğer veri setlerine oranla fazla olmasının etkili olduğu gözlenmektedir.



Şekil 5. Güvenlik Boyutu Sayısına Göre Erişim Düzeyi Başarı Oranı

4.2.2. Rol Tabanlı Erişim Kontrol Modelinin Performans Sonuçları

Rol Tabanlı Erişim Kontrol modelinin, sağlık, eğitim ve kamu veri setleri üzerindeki test sonuçları Tablo 7'da gösterilmiştir. Bu model ile, Sağlık veri seti için %92,17 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %90,63'ünde erişim düzeylerinin doğru tespit edildiği, Eğitim veri seti için %89,09 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %85,98'inde erişim düzeylerinin doğru tespit edildiği ve Kamu veri seti için %89,42 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %82,77'sinde erişim düzeylerinin doğru tespit edildiği test edilmiştir.

Çizelge 7. İzin ve Erişim Düzeyi Performansı (RBAC)

	Erişim İzni	Erişim Düzeyi
Sağlık Veri Seti	92,17%	90,63%
Eğitim Veri Seti	89,09%	85,98%
Kamu Veri Seti	89,42%	82,77%

RBAC modelinin sunduğu sonuçlar değerlendirildiğinde, modelin daha az kullanıcı ve nesneden oluşan Sağlık veri setinde %90 ve üzerinde doğru erişim izni ve erişim düzeyi sunduğu, özellikle kullanıcı ve nesne sayısı arttıkça erişim düzeyindeki doğruluk oranında azalma gözlendiği test edilmiştir.

4.2.3. Geleneksel Erişim Kontrol Modelinin Performans Sonuçları

Geleneksel Erişim Kontrol modelinin, sağlık, eğitim ve kamu veri setleri üzerindeki test sonuçları Tablo 8'da gösterilmiştir. Bu modele ait test sonuçlarında, MAC ve DAC modellerinden hangi modelin erişim izni ve erişim düzeyi oranı diğerine göre yüksek ise değerlendirmede o modelin performans yüzdesi baz alınmıştır. Bu model ile, Sağlık veri seti için %87,60 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %86,02'sinde erişim düzeylerinin doğru tespit edildiği, Eğitim veri seti için %84,79 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %81,39'unda erişim düzeylerinin doğru tespit edildiği ve Kamu veri seti için %84,21 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %79,54'ünde erişim düzeylerinin doğru tespit edildiği test edilmiştir.

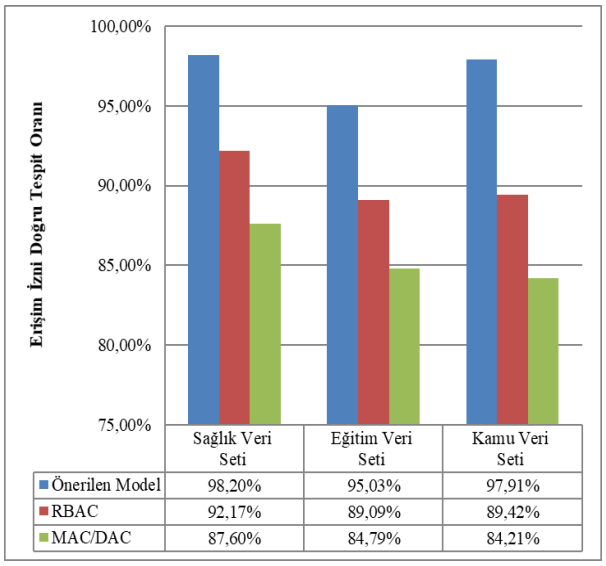
MAC/DAC modellerinin sunduğu sonuçlar değerlendirildiğinde, tıpkı RBAC modelinde olduğu gibi bu modelin de daha az kullanıcı ve nesneden oluşan Sağlık veri setinde daha yüksek oranlarda doğru erişim izni ve erişim düzeyi sunduğu, özellikle kullanıcı ve nesne sayısı arttıkça erişim izni ve erişim düzeyindeki doğruluk oranlarında azalma gözlendiği test edilmiştir.

Çizelge 8. İzin ve Erişim Düzeyi Performansı (MAC/DAC)

	Erişim İzni	Erişim Düzeyi
Sağlık Veri Seti	87,60%	86,02%
Eğitim Veri Seti	84,79%	81,39%
Kamu Veri Seti	84,21%	79,54%

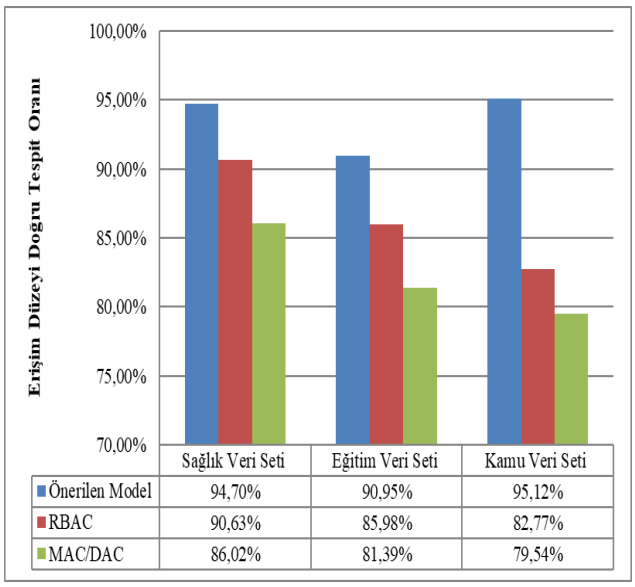
4.2.4. Performans Değerlendirme

Önerdiğimiz modelin, diğer tekniklere oranla erişim izni ve erişim düzeyi tespitinde daha başarılı sonuçlar verdiği, Şekil 6 ve Şekil 7'de görüleceği üzere özellikle her üç veri setinde de %90 ve üzerinde doğru tespit etme oranını yakaladığı, diğer tekniklerin ise kullanıcı ve nesne sayısı yüksek veri setlerinde daha az başarılı olduğu, bu durum modelimizin diğer teknikler karşısında farklı sektör uygulamaları için daha genişletilebilir ve aynı sektör uygulamaları için de daha ölçeklenebilir bir teknik sunduğunu söyleyebiliriz.

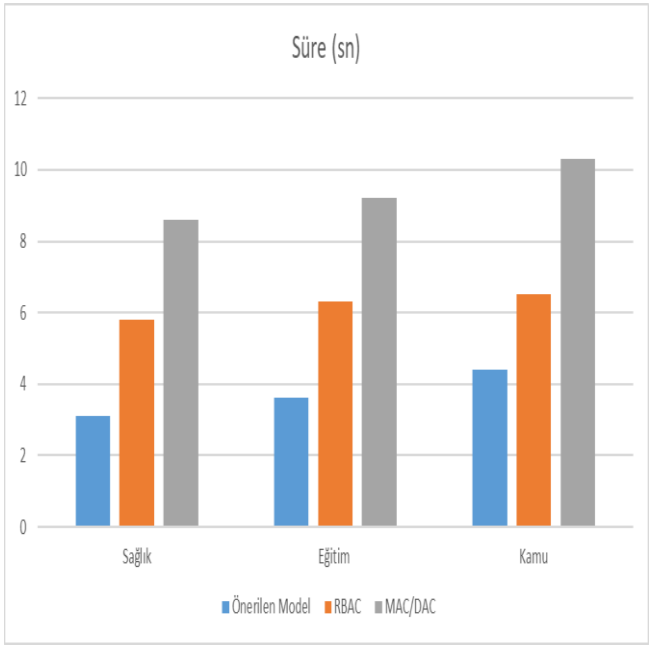


Şekil 6. Her Üç Modele Ait Erişim İzni Doğru Tespit Oranı

Şekil 8'de önerilen model ile diğer yöntemlerin süre açısından performansları gösterilmiştir. Süre olarak önerilen model ile diğer yöntemler karşılaştırılmıştır. Önerilen model her üç veri setinde de daha kısa sürede ve daha başarılı sonuçlar üretmiştir. Önerilen model doğruluk, süre ve bellek açısından karşılaştırdığımızda diğer yöntemlere göre daha başarılı sonuçlar vermiştir.



Şekil 7. Her Üç Modele Ait Erişim Düzeyi Doğru Tespit Oranı



Şekil 8. Her üç modelin zaman açısından performans değerleri

5. Sonuçlar

Çalışmada ele aldığımız önerilen yeni erişim kontrol modeli, gerçek bir dağıtık sistem üzerinde uygulanmış, böylece farklı fiziksel ortamlarda saklanan verilere kim tarafından ve hangi erişim izni ve düzeyi ile erişebileceğine yönelik hesaplamalar 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.

Çalışmanın devamında, önerdiğimiz model geliştirilerek tasarımında erişim süresini, erişim yerini ve kullanıcının davranışlarını da esas alan yeni bir çerçeve sunulacaktır.

6. Kaynaklar

Andress, J., 2011, The Basics of Information Security Understanding the Fundamentals of InfoSec in Theory and Practice, 2nd Elsevier Inc., USA, 17-49.

Angin, P., Bhargava, B. and Ranchal, R. 2019. Big Data Analytics for Cyber Security. *Security and Communication Networks.*

Behera, P. K. and Khilar, P. M.. 2016. A Novel Trust Based Access Control Model for Cloud Environment. *Proceedings of the International Conference on Signal, Networks, Computing, and Systems, Springer,* 285-295.

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

Elmagarmid, A., Rusinkiewics, M. and Sheth, A., 1999, Management of Heterogeneous and Autonomous Database Systems, 1st Morgan Kaufmann Publishers Inc., San Francisco, California, 1-41.

Huh, J. H. 2016. Next-Generation Access Control for Distributed Control Systems. *IEEE Internet Computing,* **20**(5), 28-33.

Kotari, M., Chiplunkar, N. N., and Nagesh, H. R., 2016. Framework of security mechanisms for monitoring adaptive distributed systems. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 25–36.

Kotari M. and Chiplunkar, N., 2020. Investigation of Security Issues in Distributed System Monitoring. *Information Sciences, Springer,* **2020**, 609-634.

Li, J., Liao, Z., Zhang, C. and Shi, Y. 2016. A 4D-Role Based Access Control Model for Multitenancy Cloud Platform. *Mathematical Problems in Engineering.*

Lu, R., Rahulamathavan, Y., Zhu, H., Xu, C. and Wang, M. 2016. Security and Privacy Challenges in Vehicular Cloud Computing. *Mobile Information Systems.*

Pandey, S., Dwivedi, A., Pant, J. and Lohani, M. 2016. Security enforcement using TRBAC in cloud computing. *International Conference on Computing, Communication and Automation (ICCCA), IEEE,* India, 1232-1238.

Reid, J., Cheong, I., Henrickson, M. and Smith, J., 2014. A novel use of RBAC to protect privacy in distributed health care information systems. *ACM Transactions on Information and System Security*.

Shin, M. S., Jeon, H. S., Ju, Y. W., Lee, B. J. and Jeong, S. P., 2015. Constructing RBAC Based Security Model in u-Healthcare Service Platform. *The Scientific World Journal*.

Solomon, M. G. and Kim, D., 2016, Fundamentals of Information Systems Security, 3rd ed, Jones & Bartlett Learning, Burlington, USA, 1-50.

Srivastava, K. and Shekokar, N. 2020. Machine Learning Based Risk-Adaptive Access Control System to Identify Genuineness of the Requester*, Springer*, 129-143.

Szczypiorski, K., Wang, L., Luo, X. and Ye, D. 2018. Big Data Analytics for Information Security. *Security and Communication Networks*.

Thuraisingham, B. H., 1997, Data Management Systems: Evolution and Interoperation, 1st CRC Press, Boca Raton, New York, 1-255.

Özsu, M. T. and Valduriez, P. 2011. Principles Of Distributed Database Systems. *Springer Science Business Media LLC*., USA.

Whitman, M. E. and Mattord, H. J., 2021, Principles Of Information Security, 7th Course Technology, Cengage Learning, USA, 1-527.