T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DAĞITIK VERİTABANI SİSTEMLERİ İÇİN ÖLÇEKLENEBİLİR VE GENİŞLETİLEBİLİR YENİ ERİŞİM DENETİMİ MODELİ

Mehmet GÜÇLÜ

DOKTORA TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Danışman

Dr. Öğr. Üye. Mustafa Utku KALAY

Aralık, 2020

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DAĞITIK VERİTABANI SİSTEMLERİ İÇİN ÖLÇEKLENEBİLİR VE GENİŞLETİLEBİLİR YENİ ERİŞİM DENETİMİ MODELİ

Mehmet GÜÇLÜ tarafından hazırlanan tez çalışması 04.12.2020 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Programı **DOKTORA TEZİ** olarak kabul edilmiştir.

Dr. Öğr. Üye. Mustafa Utku KALAY

Yıldız Teknik Üniversitesi

Danışman

Jüri Üyeleri

Dr. Öğr. Üye. Mustafa Utku KALAY, Danışman
Yıldız Teknik Üniversitesi _____

Prof. Dr. Oya KALIPSIZ, Üye
Yıldız Teknik Üniversitesi _____

Dr. Öğr. Üye. Yunus Emre SELÇUK, Üye
Yıldız Teknik Üniversitesi _____

Doç. Dr. Atakan KURT, Üye
İstanbul Üniversitesi - Cerrahpaşa _____

Prof. Dr. Selim AKYOKUŞ, Üye
İstanbul Medipol Üniversitesi _____

Danışmanım Dr. Öğr. Üye. Mustafa Utku KALAY sorumluluğunda tarafımca hazırlanan DAĞITIK VERİTABANI SİSTEMLERİ İÇİN ÖLÇEKLENEBİLİR VE GENİŞLETİLEBİLİR YENİ ERİŞİM DENETİMİ MODELİ başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Mehmet GÜÇLÜ

İmza

Değerli Aileme,

Sevgili Eşime,

Biricik Kızıma,

ve

Kıymetli hocam merhum Doç. Dr. Veli HAKKOYMAZ anısına.

TEŞEKKÜR

Bu tez çalışmamda, bilgi ve tecrübeleriyle çalışmalarıma yön veren, çalışmamın her anında desteğini hiçbir zaman esirgemeyen kıymetli hocam merhum Doç. Dr. Veli HAKKOYMAZ'a ve tezime katkı sağlayan değerli hocalarım Dr. Öğr. Üye. Mustafa Utku KALAY, Prof. Dr. Oya KALIPSIZ ve Doç. Dr. Atakan KURT'a;

Deneysel çalışmalarıma kaynak teşkil eden veri setlerini toplamında ve kullanımında çaba sarfeden ilgili kurum ve kuruluşlarda çalışan büyüklerime, lisans, yüksek lisans ve doktora öğrenimim süresince engin bilgi ve tecrübelerinden istifade ettiğim tüm kıymetli hocalarıma, bu stresli ve zorlu süreçte her daim yanımda olan, desteğini ve katkısını benden esirgemeyen değerli arkadaşım Çiğdem BAKIR'a;

Özellikle tez aşamasında her daim beni cesaretlendiren, teşvik eden, sabır gösteren, maddi ve manevi destekleyen eşime, biricik kızıma, anneme, babama ve kardeşlerime; şükranlarımı sunuyorum.

Mehmet GÜÇLÜ

İÇİNDEKİLER

SİMGE LİSTESİ

ED	Erişim Düzeyi
GB	Güvenlik Boyutu
İD	İzin Düzeyi
K	Kullanıcı
N	Nesne

KISALTMA LİSTESİ

ABAC	Öznitelik Tabanlı Erişim Denetimi
BT	Bilgi Teknolojisi
DAC	İsteği Bağlı Erişim Denetimi
DDBMS	Dağıtık Veritabanı Yönetim Sistemi
DKS	Dağıtık Kontrol Sistemi
EKS	Endüstriyel Kontrol Sistemi
MAC	Zorunlu Erişim Denetimi
RBAC	Rol Tabanlı Erişim Denetimi
ORAC	Nesneye Özgü Rol Tabanlı Erişim Denetimi

ŞEKİL LİSTESİ

TABLO LİSTESİ

ÖZET

Dağıtık Veritabanı Sistemleri İçin Ölçeklenebilir Ve Genişletilebilir Yeni Erişim Denetimi Modeli

Mehmet GÜÇLÜ

Bilgisayar Mühendisliği Anabilim Dalı

Doktora Tezi

Danışman: Dr. Öğr. Üye. Mustafa Utku KALAY

Günümüzde bilgiye erişim süreçlerinin güvenli bir şekilde yönetilmesi ve işletilmesi önemli bir hale gelmiştir. Bilgi sistemlerinde güvenlik unsurlarının (gizlilik, bütünlük, erişebilirlik) sağlanması, bilginin işlenmesi ve dağıtık bir yapı üzerinden paylaşımı süreçleri ancak iyi tasarlanmış bir erişim denetimi modeli ile mümkündür. Birçok kurum ve kuruluş, organizasyon yapısına uyumlu olarak tanımladığı güvenlik politikalarına dayalı farklı erişim denetimi modellerini kullanmaktadır. Erişim denetimi, sistemde tanımlı kullanıcıların yetkileri çerçevesinde bilgi kaynaklarını kullanmalarını sağlama ve böylece tüm kaynakları koruma altına alma süreçlerinden oluşur. Bilgi paylaşımını dağıtık yapılar üzerinden yapan birçok kurum ve kuruluş için ise bu süreçleri yönetmek oldukça güç ve maliyetli bir iştir. Nitekim farklı sunucular üzerinde paylaşılan ve biri diğerine mantıksal olarak bağlı olan kaynaklara ulaşmak isteyen kullanıcıların tanımlanması ve doğrulanması, kullanıcıların yetkilendirilmesi ve eylemlerinin izlenebilmesi koşulları her zaman etkin bir şekilde yapılandırılamamaktadır. Bu nedenle erişim denetimi modelleri ve süreçleri yeterince nitelikli bir biçimde gerçekleştirilememektedir. Bu tez çalışmasında önerdiğimiz erişim denetimi modeli ile, dağıtık veritabanı sistemlerinde tanımlı tüm kullanıcıların nesneler

üzerindeki izin ve erişim düzeylerinin dinamik olarak hesaplanması, böylece kullanıcıların hangi nesneyi kullanabileceklerine daha etkin bir şekilde karar verilmesi ve ihtiyaç duymadıkları bilgiye erişim yapmalarının ise engellenmesi amaçlanmıştır. Çalışmada önerdiğimiz geliştirilmiş model, Sağlık ve Eğitim hizmetleri sunan ve bir kamu hizmeti veren kurum ve kuruluşlardan alınmış gerçek veri kümeleri üzerine uygulanmıştır. Önerilen model ile birlikte tüm modeller özel bir ağda kaynak paylaşımı yapan sunucular üzerinde çalıştırılmıştır. Önerilen modelin performansı, sektör uygulamalarında çok sık rastlanan Rol Tabanlı Erişim Denetimi (RBAC), Öznitelik Tabanlı Erişim Denetimi (ABAC) ve Zorunlu (MAC) ve İsteği Bağlı Erişim Denetimi (DAC) modellerinin performansları ile karşılaştırılmıştır. Deneysel sonuçlar değerlendirildiğinde, önerdiğimiz modelin dağıtık veritabanı sistemlerine genişletilebilir olmasının yanında, yerleşik erişim denetimi modellerine kıyasla daha doğru izin ve erişim düzeyi sonuçlarını veren ölçeklenebilir bir erişim denetimi modeli sunduğu test edilmiştir.

Anahtar Kelimeler: Bilgi güvenliği, erişim denetimi, yetkilendirme, yetki seviyesi politikası, veri güvenliği, gizlilik, dağıtık sistemler.

ABSTRACT

Scalable and Expandable New Access Control Model for Distributed Database

Mehmet GÜÇLÜ

Department of Computer Engineering

Doctor of Philosophy Thesis

Advisor: Dr. Öğr. Üye. Mustafa Utku KALAY

Nowadays, it has become important to manage and operate access processes securely. Providing security elements (confidentiality, integrity, accessibility) in information systems, processing and sharing the information over a distributed structure is only possible with a well-designed access control model. Many institutions and organizations use different access control models based on security policies that they define in accordance with the organizational structure. Access control consists of the processes of enabling the users defined in the system to use information resources within the framework of their authorization and thus protecting all resources. For many institutions and organizations that share information through distributed structures, managing these processes is a very difficult and costly task. As a matter of fact, the conditions for identifying and authenticating users who want to access resources shared on different servers and logically connected to the other, authorizing users and monitoring their actions cannot always be effectively configured. For this reason, access control models and processes cannot be performed adequately. With the access control model in this thesis, it is aimed to dynamically calculate the permission and access levels of all users defined in distributed database systems, so that users can decide which

object they can use more effectively and prevent them from accessing information they do not need. The improved model in the study is applied on real data sets from institutions and organizations providing Health and Education services and a public service. With the proposed model, all models have been run on servers sharing resources in a private network. The performance of the proposed model has been compared with the performances of Role Based Access Control (RBAC), Attribute Based Access Control (ABAC) and Mandatory Access Control (MAC) and Discretionary Access Control (DAC) models, which are very common in industry applications. When the experimental results were evaluated, it was tested that the proposed model is extensible to distributed database systems, as well as providing a scalable access control model that gives more accurate permission and access level results compared to settled access control models.

Keywords: Information security, access control, authorization, authority-level policy, data security, privacy, distributed systems.

1
GİRİŞ

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 ihtiyaç duyulan süre boyunca ulaşılabilir ve kullanılabilir olmasıdır. Şekil 1.1'de bilgi güvenliğini sağlamak için bu üç temel unsurlarla korunması gösterilmiştir.

Şekil 1.1 Bilgi güvenliğinin üç temel unsuru

Genel olarak tehditlerin çoğunlukla sistemlerin güvenlik açıklarından ya da zafiyetinden faydalanılarak saldırıya dönüştüğünü, bu amaç doğrultusunda gerçekleşen saldırıların bilgi sistemlerine zarar vermesinin önlenmesi için Şekil 1.1'deki temel unsurların tamamını birlikte sağlamanın büyük bir 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.

Günümüzde bilgi sistemlerine ve kaynaklarına zarar veren yeni ve oldukça etkili olan tehditler vardır: zırhlı virüsler (armored virus), fidye yazılımları (ransomware) ve kötücül kripto – kilitleyici yazılımlar (cryptolocker malware) [2]. Sistemleri bu tür zararlı tehditlere karşı korumak için alınmış birçok gelişmiş

teknolojiler ile desteklenen tedbirler bulunmasına rağmen saldırganların çoğu zaman başarılı olabildikleri görülmektedir. Gizlilik, bütünlük ve erişilebilirlik unsurlarından en az birinin ihlal edilmesine neden olabilecek türden ortaya çıkabilecek herhangi bir olay, durum ya da olası riskler bir güvenlik ihlali olarak değerlendirilir [3]. Bazı ihlaller kasten sistemleri erişilemez kılıp hizmetleri sekteye uğratırken, bazıları ise öngörülemeyen hatalar nedeniyle kazaen oluşur. Güvenlik ihlalleri ister kazaen 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, kaza sonucu veya kasten oluşan veri değişiklikleri gelmektedir [2, 4]. Kasten veya kazaen değiştirilen veriler, özellikle bilişim sistemleri güvenliğinin bütünlük ilkesini doğrudan etkiler ve bir güvenlik ihlalinin doğmasına sebebiyet verir. Kasten veya kazaen veri değiştirme olaylarının ortaya çıkmasında kullanıcılara gereğinden fazla yetki verilmesi ve yetkilerin denetiminin zayıf tutulması durumları önemli bir rol oynar [5]. 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 denetimi 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 [6, 7, 8, 9, 10]. Bu sebeple erişim denetimi 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, genişletilebilir ve erişim denetimi işlevselliğinin tutarlı bir şekilde tasarlanmış olmasının da büyük önem taşıdığı gözlenmektedir.

1.1 Literatür Özeti

Dünyada bulut bilişim teknolojisi, bilgi ve iletişim teknolojileri sektörünün gelişmekte olan alanları arasında yer alır. İnternet ortamında çok sayıda bilgisayar korsanı (saldırgan) ve kırıcılar bulunduğundan, bulut bilişim ortamında çalışan uygulamaların ve muhafaza edilen verilerin güvenliğini sağlamak oldukça önemlidir. Bu amaçla son zamanlarda bulut bilişim odaklı geliştirilmiş erişim kontrol modellerinin sayısının hızla arttığı görülmektedir [11, 12, 13]. Behera, P. K. ve Khilar, P. M. [14] kullanıcı güven esasına dayanan yeni bir erişim denetimi modeli geliştirmiştir. Modelde, kullanıcılar güven değerine göre yetkilendirilir, yani hem kullanıcılar hem de bulut ortamdaki her bir kaynağın güven değeri hesaplanır. Kullanıcılar ve kaynaklar için hesaplanan güven değerleri, belirlenen eşik değerlerden yüksek ise güvenilir olarak kabul edilir. Benzer bir çalışmada ise, bulutta depolanan sınıflandırılmış veriler için yeterli derecede güvenliği sağlayan şifreleme tekniklerine dayalı ve uyarlanabilir çok düzeyli bir güvenlik çerçevesi önerilmiştir [15]. Önerilen güvenlik sistemi, bulut ortamına iyi uyum sağlar ve aynı zamanda özelleştirilebilinir, ayrıca iş gereksinimlerine ve ticari koşullara göre değişen, farklı hassasiyet gerektiren veri güvenliği seviyelerini güvenli bir şekilde gerçekleştirir.

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 [8, 10, 16]. Bir çalışmada, her erişimin en az ayrıcalık ilkesine uyan politikalara karşı kontrol edilebilmesi için Endüstriyel Kontrol Sistemi (EKS) topluluğu tarafından uyarlanabilecek bir erişim kontrol mimarisi sunulmuştur [16]. Önerilen mimaride merkezi politika yönetiminin ve bağlı her saha cihazının korunması amaçlanmıştır. Bertolissi, C. ve Fernandez, M. [17], bilgi paylaşımını dağıtık yapılar üzerinden yapan sistemlerin gereksinimleri analiz ederek yeni bir erişim denetimi tekniği geliştirmiştir. 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 [18, 19]. Havalimanı / havaalanı gözetleme, savunma sanayisi ve hastane yönetim sistemleri gibi statik erişim kontrol sistemlerinin etkin bir şekilde yönetilemediği ve işlev yönünden zayıf kaldığı birçok gerçek dünya uygulaması vardır [20]. Erişim isteğinde bulunan kullanıcıların gerçekliğine göre uyarlanan ve güveni esas alan bir sisteme ihtiyaç vardır. Rol tabanlı erişim kontrol modeli de dahil olmak üzere yerleşik erişim kontrol modellerinin birçoğu davetsiz misafirleri veya bilgisayar korsanlarını kolayca çekebilir. Yine politikaya dayalı erişim denetimi modellerinde, başlangıçta tanımlanan güvenlik politikaları dinamik olarak değiştirilemediğinden uygulamalarda uyum eksiklikleri ön plana çıkar. Srivastava, K. ve Shekokar, N. tarafından önerilen erişim kontrolü modeli, istekte bulunanın gerçekliğini tespit eden, olası riskleri hesaplayan ve risklerin niteliğine ve derecesine göre hareket eden bir teknik sunar [20]. Bu teknik, 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.

Öznitelik tabanlı erişim kontrolü (ABAC), özellikle karmaşık dinamik ortamlarda ezici bir rekabet avantajı gösteren, olağanüstü ifade ve ölçeklenebilirliğe sahip olgunlaşan bir yetkilendirme tekniğidir. Ne yazık ki, ABAC'da esnek bir istisnai onay mekanizmasının bulunmaması, mevcut uygulamaların kaynak kullanılabilirliğini ve iş zamanı verimliliğini bozarak büyümesini sınırlandırabilir [21, 22]. Xu, Y. ve arkadaşları [23], acil istisnai yetkilendirmelerdeki esnekliği artırmak ve böylece kaynak kullanılabilirliğini ve iş zamanlamasını iyileştirmek için uygun bir bulanık genişletilmiş ABAC (FBAC) tekniğini önermiştir. Çalışmada, politikalara uymayan taleplerin politika eşleştirme derecelerini değerlendirmek için bulanık değerlendirme mekanizması kullanılmıştır. Böylece önerilen teknik,

katılımsız istisnai yetkilendirmeler elde etmek için özel onay kararları verebilir. Ayrıca, riskleri azaltmak için uygun yetkileri düzenlemek amacıyla periyodik kredi düzenleme denetimi ile yardımcı bir kredi mekanizması tasarlanmıştır [23].

Bir bilgisayar sisteminde erişim kontrolü, sistemin kaynaklarına erişim izni verip vermemeye karar vermek için kullandığı mekanizmaları ifade eder. Genel olarak bilgi sistemlerinde gizlilik ve güvenlik kısıtlamalarının ve özellikle erişim kontrolünün uygun bir şekilde yönetilmesi oldukça zordur [24, 25]. Rol tabanlı erişim denetimi (RBAC) ve türevleri, bilgi teknolojileri uygulama alanlarında çok sık karşılaşılan ve yetkilendirme politikaları genel kabul gören bir yaklaşım olarak düşünülebilir. Ancak, RBAC'ın nesneye özgü uygun bir desteği yoktur. Buna karşın, öznitelik tabanlı erişim denetimi (ABAC), nitelikleri tanımlayan politikaları ve kuralları esas alan bir erişim tekniği sunar. Dezavantajı, rollerin soyutlanmasından yoksun olmasıdır. Her iki erişim denetiminde gözlemlenen bu eksiklikleri ele alan bir çalışmada, nesneye özgü rol tabanlı erişim kontrolü (ORAC) modeli sunulmuştur [25]. İlgili çalışmada ORAC, bir yandan bilgi sistemi mühendislerinin, yöneticilerinin ve kullanıcılarının iyi bilinen roller prensibini kullanmayı gerçekleştirirken, öte yandan gerektiğinde nesnelere ince taneli bir şekilde ulaşılmasını sağlar.

Literatürde son yıllarda, bugüne kadar yukarıda belirtilen amaçlar doğrultusunda farklı teknikleri kullanarak geliştirilen çeşitli erişim denetimi modelleri vardır. Bu tez çalışmasında ise bu çalışmalardan farklı olarak, kullanıcının geçmiş eylemlerine, bireyler arasındaki etkileşimlere veya güven değerine bakılmaz, tam aksine her kullanıcıya organizasyon yapısına uygun bir şekilde tanımlanmış farklı güvenlik boyutlarından birçok değer (nitelik) atanır. Dağıtık ortam kullanıcılarının erişim istekleri, istisnai durumlara (özel izinler ve yetkilendirmeler), kullanıcılara atanmış güvenlik boyutu değerlerine ve nesnenin erişim düzeylerine göre değerlendirilir. Başka bir deyişle erişim izinleri, boyut değerleri ve erişim düzeyi ("Okuma/Yazma", "Yalnızca Okuma", "Yalnızca Yazma", "Örtülü" veya "Yok") ile ilişkilendirilir. Her güvenlik boyutundan en az kısıtlayıcı erişim ya da izin düzeyi alınır ve farklı güvenlik boyutlarından gelen düzeyler ile karşılaştırılır, ilişkili

düzeyler arasından en fazla kısıtlayıcı erişim ya da izin düzeyi esas alınarak genel erişim izni veya düzeyi dinamik olarak hesaplanır.

1.2 Tezin Amacı

Literatürde erişim denetimlerine yönelik yapılan araştırma çalışmalarının sadece belirli alanlar üzerine yoğunlaştığı, bu alanda son yapılan araştırmaların ise daha çok bulut bilişim (cloud computing), büyük veri (big data) ve nesnelerin interneti (IoT) konularını kapsadığı gözlenmektedir [26, 27, 28]. Özellikle dağıtık veritabanı sistemleri üzerine yapılan çalışmaların çok sınırlı bir sayıda kaldığı, bu çalışmalarda ise mevcut erişim denetimi modellerinin farklı dağıtık veritabanı sistemlerine uyarlanmasında birtakım güçlükler yaşandığı, yönetilebilir bir erişim denetimi modeline doğru ilerlemelerde ciddi maliyetlerin ortaya çıktığı, farklı sektör uygulamalarında alışagelmiş erişim denetimi modellerinin dağıtık veritabanı sistemlerinde beklenen etkiyi yaratmadığı, en önemlisi ise kaynakların kullanımı ve paylaşımı konusunda gerekli olan dinamizme ulaşılamadığı anlaşılmaktadır [8, 10, 16, 17].

Her bir kuruluşun gereksinimlerine göre yapılandırılan birkaç farklı erişim denetimi modeli vardır. Erişim denetimi modelleri genellikle 3 ana kategori altında toplanmıştır: Rol Tabanlı Erişim Denetimi, Öznitelik Tabanlı Erişim Denetimi ve Geleneksel Erişim Denetimi (İsteğe Bağlı Erişim Kontrolü ve Zorunlu Erişim Kontrolü) [3]. Rol Tabanlı Erişim Denetimi modeli ve türevlerinin, daha dinamik ve değişme eğiliminde olan sistemler için etkili olmadığı birçok gerçek dünya uygulaması vardır. Aynı durum Öznitelik Tabanlı Erişim Denetimi ve Geleneksel Erişim Denetimi modelleri için de geçerlidir [20, 25]. Mevcut erişim denetimi modelleri organizasyonel yapısı karışık olan, kullanıcı ayrıcalıkları ve iş fonksiyonları tam olarak ayrılmamış organizasyonlarda uygulanması oldukça güç olabilmektedir ve mevcut uygulamaların kaynak kullanılabilirliğini ve iş zamanı verimliliğini bozarak büyümesini sınırlandırabilmektedir [20, 21, 22, 25].

Bu tez çalışmasında, sektör uygulamalarında sık karşılaşılan ve araştırmalara konu edilen bazı problemler ele alınarak, farklı sektör uygulamalarına uyarlanabilir ve birçok dağıtık veritabanı sistemlerinde ölçeklenebilir, güvenli ve mevcut erişim denetimi modellerine kıyasla daha tutarlı erişim düzeyi sonuçlarını sunabilen

dinamik bir erişim denetimi modeli geliştirilmiştir. Çalışmanın bilimsel katkısı olarak, önerilen model ile dağıtık veritabanı sistemlerinde aktif rol alan tüm kullanıcıların nesneler üzerindeki izin ve erişim düzeylerinin doğru bir şekilde hesaplanması, gereğinden fazla yetkilendirmeden kaçınılarak kullanıcıların hangi nesneye erişim yapabileceklerine daha dinamik bir şekilde karar verilmesi ve ihtiyaç duymadıkları bilgiye erişim yapmalarının engellenmesi, böylece hatalı ya da gereğinden fazla yetkilendirmeden kaynaklı oluşabilecek güvenlik ihlallerinin önüne geçilerek veri güvenliğinin etkin bir şekilde sağlanması amaçlanmıştır.

1.3 Hipotez

Tezin hipotezleri aşağıdaki gibi listelenebilir:

- Dağıtık veritabanı sistemlerinde, tüm kullanıcı ve nesneler (kaynaklar, veriler) farklı organizasyon yapılarına uygun bir biçimde sınıflandırılabilinir ve kullanıcı ve nesnelere farklı güvenlik boyutlarında birçok değer atanabilinir.
- Kullanıcılara farklı erişim düzeylerinde özel hak ve yetki verilerek kaynakların kullanılabilirliliği ve paylaşımı güvenli ve kontrollü bir şekilde artırılabilinir, istisnai bir onay mekanizması işletilerek sektör uygulamalarına esneklik kazandırılabilinir.
- Başlangıçta karar verilen güvenlik politikaları dinamik olarak değiştirilebilinir, böylece değişen ticari koşullara ve iş gereksinimlerine uyum sağlanabilinir.
- Erişim denetimi modelinde, hem kullanıcılar hem nesneler birlikte rol alabilir, kullanıcılara ve nesnelere farklı güvenlik boyutlarında atanan değerlere göre erişim izinleri ve erişim düzeyleri (okuma, yazma, yalnızca okuma, vb.) hesaplanabilinir.
- Geliştirilecek dinamik bir erişim denetimi modeli ile, hatalı ya da gereğinden fazla yetkilendirmeden kaynaklı oluşabilecek güvenlik ihlallerinin önüne geçilmesi ve veri güvenliğinin etkin bir şekilde sağlanması gözlemlenebilinir.

- Farklı sektör uygulamalarına genişletilebilir ve iş gereksinimlerine ve hacmine / büyüklüğüne göre ölçeklenebilir yapıda bir erişim denetimi modeli geliştirilebilinir.
- Dağıtık veritabanı sistemlerinde veri erişimi, geliştirilecek erişim denetimi modeli kullanılarak dinamik bir şekilde denetlenebilinir.
- Veri erişim sürelerini ve gecikmeyi azaltmak için kullanıcının geçmiş izin ve erişim düzeyi sonuçları kullanılabilir.

2
BİLGİ SİSTEMLERİ GÜVENLİĞİNİN TEMELLERİ

2.1 Bilgi Sistemleri Güvenliği

Bilgi sistemleri güvenliği, bilgi teknolojisi (BT) alanında bilgisayarları, ağları ve kullanıcılarını korumaya odaklanan geniş bir konudur. Birçok kurum ve kuruluş, bilgi teknolojileri sistemlerine yönelik birtakım riskleri yönetmek ve olası tehditlere karşı ileri düzeyde önlemler almak için Bilgi Sistemleri Güvenliğinin (ISS) en iyi uygulama alanlarını benimsemek zorunda kalır. Bilgisayarları ya da cihazları internete bağlamak bir anlamda onları saldırıların hedefi haline sokmaktadır. Özellikle dijital ürünler iş ve ticaret hayatında gerekli hale geldiği müddetçe, artan saldırıların da hedefi haline gelecektir [29]. Bu tür saldırılar ve tehditler, bir veritabanı saldırısında özel bilgilerin çalınması, makineye kötü amaçlı yazılım yüklenmesi ve kasıtlı hizmet kesintileri dahil olmak üzere tüm şekil ve boyutlarda ortaya çıkabilir [30].

Bilgi sistemlerini ve üzerlerindeki veriyi koruma faaliyetleri için kuruluşlar çeşitli güvenlik araçları arasından seçim yapabilir. Bu güvenlik araçlarından en yaygın kullanım alanına sahip olanlar, bu bölümde ele alınacak olan genel bir bilgi güvenliği politikasının parçası olarak kullanılabilir.

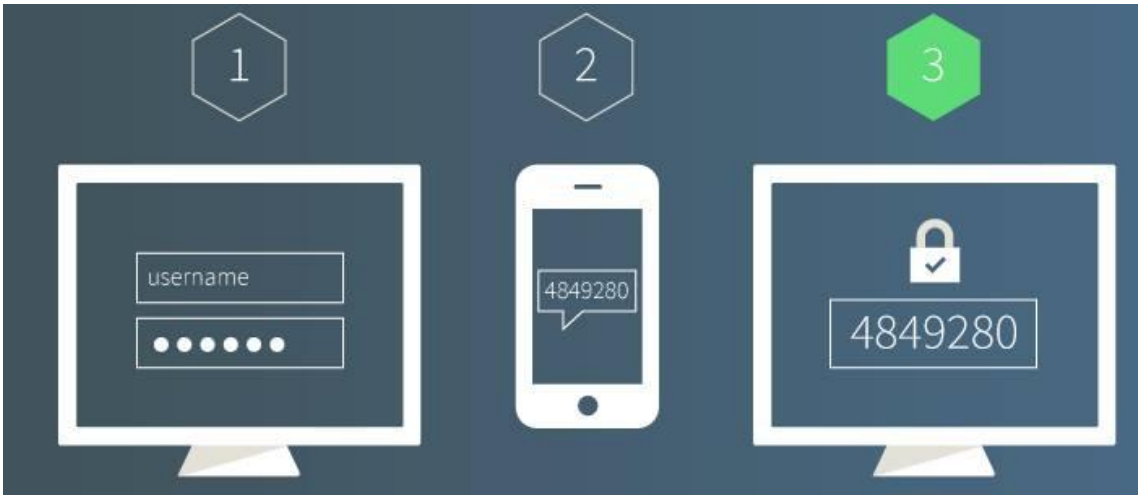
2.1.1 Kimlik Doğrulama

Kimlik doğrulama, bir kişinin veya bir şeyin aslında kim veya ne olduğunu belirleme işlemidir. Günümüzde en yaygın kimlik doğrulama şekli kullanıcı kimliği (ID) ve şifredir [31]. Kullanıcı kimlik doğrulaması, bir ağa ya da internete bağlı sistemlerde ve sistem uygulamalarında, kaynaklara erişim sağlamak için işletim sistemlerinde ve uygulamalarında, kablolu ve kablosuz ağlarda ve benzeri platformlarda insan ve makine etkileşimlerine izin verir. Örneğin kurumsal web sitelere giriş yapan kullanıcıların doğrulanması işlemi kimlik doğrulama yöntemi ile gerçekleştirilir. Yani erişim elde etmek için, kullanıcıların web sitesine söyledikleri kişi olduklarını kanıtlamaları gerekir. Kimlik ve şifre, kullanıcının

kimliğini doğrulamak için yeterlidir, bu da sistemin kullanıcıyı yetkilendirmesine izin verir [32]. Yetkilendirme işlemi, bir sistem ya da uygulama ekranında oturum açan kullanıcıların neyi görebileceğini ve hangi işlemleri gerçekleştirebileceğini belirleyen şeydir.

Açıkça ifade etmek gerekirse, kullanıcı kimlik doğrulamasının üç ana görevi vardır [31]:

- İnsan (kullanıcı) ile makine (sunucu, bilgisayar) arasındaki bağlantıyı yönetir.
- Kullanıcı kimlik doğrulamasını gerçekleştirir.
- Kullanıcının yetkilendirme aşamasına geçebilmesi için sistemin kimlik doğrulamayı onaylamasını veya reddetmesi sağlar.



Şekil 2.1 İki faktörlü kimlik doğrulama

Şekil 2.1'de görüldüğü gibi, kullanıcı kimlik bilgilerini bir web sitenin giriş formuna girer. Ekrana girilen bilgi, kimlik doğrulama sunucusuna gönderilir ve tüm kullanıcı kimlik bilgileri ile karşılaştırılır. Bir eşleşme bulunursa eğer, sistem kullanıcıya yetki verir ve hesaba erişmesine izin verir. Bir eşleşme bulunmaz ise, sistem kullanıcıdan kimlik bilgisini tekrar girmesini ve tekrar denemesini ister.

Kullanıcı kimlik doğrulamasını tam olarak anlamak çok önemlidir, çünkü kimlik doğrulama yetkisiz kullanıcıların hassas bilgilere erişmesini önleyen bir süreçtir [32]. Kimlik doğrulama, bir kullanıcının yalnızca ihtiyaç duyduğu bilgilere

erişmesini ve başka bir kullanıcısının ise hassas bilgileri görememesini sağlar. Kullanıcı kimlik doğrulama sistemi güvenli olmadığında, saldırganlar istedikleri bilgileri alarak sistemi aşıp erişim sağlayabilirler. Veri ihlallerinin kurbanı olan Yahoo, Equifax ve Adobe gibi web siteleri, web sitelerin güven altına alınmadığında ne olduğuna dair en iyi örneklerdir [33].

Kimlik doğrulaması için, bir kullanıcının sadece kullanıcı tarafından bilinen ve sunucu ortamında muhafaza edilen özel bilgileri sağlaması gerekir. Bu bilgiler, kimlik doğrulama faktörü olarak adlandırılır ve üç ana türü vardır [34]:

- ***Bilgi Faktörü:*** Bir kullanıcının oturum açmak için ihtiyaç duyduğu bilgileri içeren faktördür. Örneğin, kullanıcı adı, parola, tek kullanımlık şifre gibi unsurlar bilgi faktörü kapsamındadır. Bu faktörün dezavantajı, güvenlik açısından zayıf olmalarıdır, çünkü bu bilgiler paylaşılabilir veya tahmin edilebilir niteliklere sahiptir.
- ***Sahip Olunan Faktörler:*** Kullanıcının oturum açmak için sahip olması gereken her şey, sahip olma faktörü olarak bilinir. Tek kullanımlık şifre, kimlik kartları, akıllı anahtar, fiziksel belirteçler vb. tümü sahip olma faktörleri olarak kabul edilir.
- ***Kalıtsal Faktörler:*** Kişinin biyolojik özelliklerinin kullanıldığı faktördür. İris, parmak izi, el tanıma ve yüz tanıma gibi biyometrik teknikler bu kategoriye girer.

Kimlik doğrulama işlemi iki kategoride değerlendirilebilir: şifreli ve şifresiz seçenekler [35].

1) Şifreli Giriş Sistemleri

Çoğu kullanıcı şifreleri seçenekleri bilmektedir. Şifreli seçenekler, internetin ilk çıktığı zamandan bu yana kimlik doğrulaması için kullanılan temel bir yöntem olmuştur. Şifreleme tekniğine dayanan kimlik doğrulama süreçleri genellikle şöyle ifade edilir [35]:

- Bir web kaynağının ya da sistemin giriş ekranına gelindiğinde, kullanıcı adı ve şifre bilgileri girilmesi istenir.

- Kullanıcı adı ve şifre bilgileri ilgili ekrana girildikten sonra bilgiler sunucuya gönderilir ve buradaki bilgiler ile karşılaştırılır.
- Bir eşleşme bulunduğunda, hesap bilgisi doğrulanmış olur ve o hesaba giriş için izin verilir.

Kullanıcı hesaplarını güvence altına almak için bir şifre tek başına yeterli olarak görünse de, çoğumuz çevrimiçi kullanıcı hesaplarında hassas bilgileri depolarız. Birçok kullanıcı, parola oluşturma konusunda genellikle kolay olanı tercih eder. Yani güçlü şifreler oluşturmak yerine, kullanıcılar hatırlanması daha kolay olduğu için basit bir harf, sayı ve simge düzeni kullanır. Bir araştırmada, kullanıcıların yaklaşık % 54'ünün hesaplarında 5 veya daha az farklı şifre kullandığını tespit etmiştir [36]. Bu durum ve daha fazlası güvenliğin azalmasına, riskin de artmasına neden olur. Çünkü saldırganlar, kullanıcıların oturum açma bilgilerini tahmin edebilir veya bir eşleşme bulunana kadar muhtemel tüm kombinasyoları test etmek için gelişmiş birçok teknikleri kullanabilir [36].

2) Şifresiz Giriş Sistemleri

Basitçe söylemek gerekirse, şifresiz bir giriş sistemi, şifre gerektirmeyen bir kimlik doğrulama yöntemidir. Son birkaç yıldır, bu tür kimlik doğrulama yöntemleri daha popüler hale geldi [32]. Birkaç farklı şifresiz giriş türü vardır. Bunlardan en yaygın olan iki türü: *E-Posta Kimlik Doğrulaması* ve *Biyometrik'tir*.

a) E-Posta Kimlik Doğrulaması

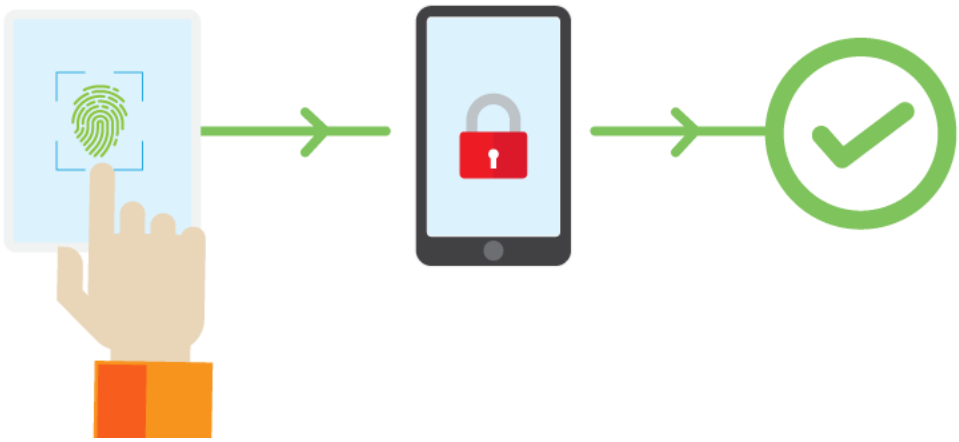
En yaygın kullanılan şifresiz kimlik doğrulama türlerinden biridir. Bir e-posta hesabına sahip olan herkesin kullanabileceği basit bir yöntemdir. Bu yöntemle, kullanıcılar kolayca bir hesap oluşturabilir, hesaba giriş yapabilir ve tek bir tıklamayla ödeme yapabilirler [32].

Şekil 2.2 E-posta kimlik doğrulaması

Şekil 2.2'de örnek bir e-posta kimlik doğrulama yöntemi gösterilmiştir. E-posta gönderilerek, kullanıcıların giriş yapma istekleri onaylanır. İstek, güvenlik protokollerinin her birini geçtikten sonra kullanıcılar hesaplarına erişebilir.

b) Biyometrik

Parmak izi ve iris taraması, yüz tanıma ve biyolojik özelliklerle diğer doğrulama türleri biyometri kategorisine girer. Biyometrik kimlik doğruma türü en güvenli yöntemlerden biri olarak kabul görür, çünkü biyometrik özellikler benzersizdir ve çoğaltılması oldukça zordur [37]. Biyometrik özelliğin bir diğer avantajı da kullanımının kolay ve anlaşılır olmasıdır. Örneğin, parmak izi kimlik doğrulamasında kullanıcının yalnızca sistemde tanımlı olan parmağını tarayıcıya okutması yeterlidir, gerisi sistemin sorumluluğundadır.



Şekil 2.3 Parmak izi kimlik doğrulaması

Şekil 2.3'te kullanıcı sistemde tanımlı olan parmağını tarayıcıya okutur ve sistemin ona erişim izni vermesini bekler. Arka planda sistem, taranan parmak izini orijinal parmak izi baskısıyla karşılaştırır. Her iki parmak izinin eşleşmesi halinde sistem kullanıcıya erişim izni verir.

Birçok faydasına rağmen, biyometrik kimlik doğrulamanın birkaç dezavantajı da vardır. Bunlardan ilki, son çalışmalar göstermiştir ki parmak izinin kopyalanması eylemi sanıldığından çok daha kolaydır. Şayet birisi parmak izlerini çalıyorsa, bu da biyometrik kimlik doğrulama yönteminin bir daha asla güvenle kullanılamayacağını gösterir [36]. Başka bir dezavantajı ise, çevresel faktörlerden etkilenmesi ve %100 doğru sonuç vermemesidir.

2.1.2 Erişim Denetimi

Kimlik doğrulaması işlemi tamamlandıktan sonraki ilk adım kullanıcıların uygun bilgi kaynaklarına erişmesini sağlamaktır. Aynı zamanda kullanıcının kim olduğu ve neye erişebileceği belirlendikten sonra, kullanıcının kullanmaması gereken ve ihtiyaç duymayacağı herhangi bir şeye erişmesinin de aktif olarak engellenmesi gerekir. Bu, erişim denetimi kullanılarak yapılır. Erişim denetimi, kullanıcıların kaynaklar üzerindeki erişim düzeyinin belirlenmesi işidir, başka bir deyişle kullanıcıların kaynaklar üzerindeki okuma, yazma, ekleme, silme, vb. yetkilerini belirler [38]. Birkaç farklı erişim denetimi modeli vardır: Erişim Kontrol Matrisi, Erişim Kontrol Listesi, İsteğe Bağlı Erişim Denetimi Modeli, Zorunlu Erişim

Denetimi Modeli, Bell-LaPadula Modeli, Biba Bütünlük Modeli, Clark ve Wilson Modeli, Rol Tabanlı Erişim Denetimi Modeli, vd.

Erişim denetimi ve denetim modellerine bir sonraki bölümde (3. Bölüm) ayrıntılı bir şekilde değinilecektir.

2.1.3 Yetkilendirme

Bir kullanıcının kimliği doğrulandıktan sonra yetkilendirme işlemi ile, kullanıcının hangi izinlere sahip olacağı belirlenir [39]. Bir kullanıcının yetki düzeyi, kullanıcının hesabıyla ilişkili ek özellikler baz alınarak yetkilendirme kuralları dahilinde belirlenir. Yetkilendirme, erişime izin verme, erişimi sınırlama, önleme ve iptal etme karar süreçlerinden oluşur. Örneğin, üst düzey bir yöneticinin bir kullanıcıya bir web site için içerik oluşturmasına ve düzenlemesine ya da yayınlamasına izin vermek için birtakım kurallar oluşturmasına izin verebilir. Yetkilendirmede erişim izninin ve düzeyinin görev ve rol tanımlarına göre en kısıtlayıcı seviyede tutulması önem arz eder [40].

Modern bilgisayar sistemlerinde, uygulamaların paylaştırılması ve yönetiminin kolaylaştırılması için iyi tasarlanmış yetkilendirme süreçlerine ihtiyaçları vardır. Bilgisayar sistemlerinde ve ağlarda erişim denetimi, erişim politikalarına dayanır ve iki aşamadan oluşur [40]:

1) Erişim yetkisi vermek için birtakım kurallar içeren politika tanımlama aşaması.
2) Erişim isteklerine olumlu ya da olumsuz yanıt veren politika uygulama aşaması.

Yetkilendirme, önceden tanımlanan yetkilere bağlı olarak erişim taleplerinin değerlendirilmesinden önce gelen politika tanımlama aşamasının bir işlevidir [41]. Erişim kontrolü, kullanıcının kimliğini kontrol etmek için kimlik doğrulamasını da kullanır. Yetkilendirme sırasında, bir sistem kimliği doğrulanmış bir kullanıcının erişim kurallarını doğrular ve kaynak erişimine izin verir veya erişimi reddeder. Başka bir deyişle, bir kullanıcı bir kaynağa erişmek istediğinde, erişim denetimi süreci başlar ve kullanıcının bu kaynağı kullanma yetkisine sahip olup olmadığı araştırılır.

2.1.4 Şifreleme

Şifreleme, bir metnin şifre çözme anahtarı olmayan herhangi biri tarafından okunmayacak şekilde karıştırılarak şifreli metin haline dönüştürülmesi işlemidir. Şifreleme, kimlik doğrulamanın ve/veya yetkilendirmenin kaynakları yetkisiz kullanıcılardan koruyamaması durumunda kaynakları korumak için bağımsız olarak çalışabilir [42].

"şifreleme", iki aşamalı olarak yapılır: şifreleme ve şifre çözme [42]. Şifreleme, bilgileri kodlanmış şifreli bir metin haline dönüştürür ve bir şifreleme algoritması ile üretilen bir şifreleme anahtarıyla verileri paketler. Veriler, alıcısına ulaştığında uygun bir şifre çözme anahtarı (simetrik veya asimetrik anahtar) kullanılarak şifresi çözülür ve böylece kodlanmış veriler düz (açık) metne dönüştürülür. Şifrelemede ve şifre çözmede aynı anahtar kullanılmış ise buna simetrik anahtarlı şifreleme, farklı anahtar kullanılmış ise buna da asimetrik anahtarlı şifreleme denir.

Veri ihlallerine rağmen şifreleme, saldırganlar güvenlik duvarını geçse bile bir kurumun özel verilerinin güvende kalmasını sağlar. İşletmeler, giderek artan sayıda özel kullanıcı verisi topladığından, bu verilerin yetkisiz kişilerin eline geçmesini önlemek için sahip oldukları tüm verileri şifrelediklerinden emin olmaları gerekmektedir. İşletmelerin, çevrimiçi işlemler ve süreçler için veri şifrelemesine yatırım yapma çabasını göstermelerini gerektirebilecek birkaç neden sayabiliriz [43]:

1) Bilgisayar korsanları, kablosuz ağ kanallarına kolayca sızabilir ve ağ üzerinden iletilen verileri yakalayabilir. Veri şifreleme, hassas bilgilerin güvenli bir şekilde iletilmesini ve verilerin ifşa edilmemesini sağlar.
2) Saldırganlar, sürekli olarak en sıkı siber güvenlik savunmalarını aşmanın yeni yollarını öğrenirler, bu nedenle şirketlerin, güvenlik duvarları ihlal edildiğinde saldırganların verilerini okuyamayacaklarından emin olmaları gerekir. Veri şifreleme, saldırganların hassas bilgilere erişmesini engeller.
3) Güvenli olmayan (lisanssız veya sertifikasız) çevrimiçi kaynakların ve uygulamaların yüklenilmesi ve kullanılması sistemi savunmasız bırakabilir.

Nitekim güvenliği test edilmemiş uygulamalar arka planda birtakım açıklar bırakabilir. Saldırganlar uygulamaların bu açıklarından faydalanarak izinsiz girişlere ve güvenlik ihlallerine neden olabilirler. Veri şifreleme, özel verilerin karıştırılmasını ve yetkisiz kullanıcılar tarafından okunmasını engelleyerek bu ve benzeri durumları ortadan kaldırır.

4) Aynı ya da benzer faaliyet alanında yer alan şirketlerin rekabetinde, rakiplerinin iş ve ticari adımlarını öğrenebilmek için rakiplerinin önem arz eden verilerine erişmek isteme durumu gözlemlenebilir. Bu veya buna benzer davranışlar teknoloji meraklısı bireylerin ücret karşılığında şirketlerin çevrimiçi kaynaklarını hacklemesi ile bilgisayar korsanlığı işinin büyümesine yol açtı. Veri şifreleme ile, bir saldırgan veya yetkisiz kılınan bir kullanıcı güvenlik sistemlerini başarılı bir şekilde aşsa dahi hassas verileri okumayaz veya kullanamaz.

2.2 Veri Güvenliği

Veri Güvenliği, verileri yetkisiz erişimden, kazaen kayıplardan veya tahribat edilmesi gibi birtakım problemlerden korumak için belirli kontroller, standart politikalar ve prosedürler uygulamayı içerir. Ayrıca hassas verilere erişimi, manipülasyonu veya ifşayı sınırlandırmak için güvenliğin fiziksel yönünü de birleştirebilir [44]. Hemen hemen birçok kuruluşun, organizasyon yapısına uygun olarak kendine has veya genel kabul görmüş bir tür veri güvenliği denetimi vardır. Bu tür denetimler, kurumsal web siteleri, çalışan uygulamalar, ağlar, ticari veya şahsi bilgisayarlar ve sunucular, şahsi veya ticari veritabanı gibi alanlara erişimleri engellemek için birtakım güvenlik uygulamalarını da içerebilir. Hassas verilerin çalınması, kaybı, yetkisiz ifşası veya tahribatı bir kuruluş için oldukça maliyetli sonuçlar doğurabilir, hatta birtakım ticari zorlukları da beraberinde getirebilir. Veri güvenliğinin önemi de bu tür durumlarda ortaya çıkmaktadır.

Son birkaç yılda veri ihlallerinde önemli bir artış gözlenmektedir. Hem kamu sektörü hem özel sektör bu ihlallerin kurbanı olmuştur. Tablo 2.1‘de yakın geçmişte yaşanmış bazı önemli veri ilhallerine örnekler gösterilmiştir [3].

Tablo 2.1 Yakın geçmişte yaşanmış bazı veri ihlalleri

Kuruluş	Veri İhlali	Veri İhlalinin Etkisi
Adobe Systems Incorporated: Yazılım Abone Veritabanı	03.10.2013 tarihinde bilgisayar korsanlarının 150 milyon hesap bilgisini yayınladığı, şifrelenmiş müşteri kredi kartı verisini çaldığı duyurulmuştur.	3 milyon kredi kartı verisi çalınmış ve 160 bin sosyal güvenlik numarasına erişilmiştir.
Target Corp.: Ülke çapındaki perakendecinin müşteri ve kredi kartı veritabanı	Aralık 2013'te Target sistemlerinde meydana gelen bir veri ihlali 110 milyon kadar müşteriyi etkilemiştir.	Target, ihlal nedeniyle finans kuruluşlarında meydana gelen zararı karşılamayı kabul etmiştir.
Sony Pictures Entertainment: Gizli dosyalar, e-postalar ve çalışanların verisi	24.11.2014 tarihinde bir bilgisayar korsanı grubu Sony Pictures film stüdyosundan gizli bilgi sızdırmıştır. Sızdırılan bu veriler; Sony Pictures çalışanlarına ve ailelerine ait kişisel bilgiler, çalışanlar arası e-postalar, Sony yöneticilerinin maaş bilgileri, henüz gösterime girmemiş filmlerin kopyaları ve diğer bilgileri içermektedir.	ABD Başkanı Barrack Obama, bu siber saldırı sonrası Sony olayı gibi benzer siber suçlara daha iyi yanıt vermek ve vatandaşların mahremiyetini korurken bu tür suçları benzer çevrim dışı suçlarla uyumlu bir şekilde yargılayabilmek için mevcut yasaları güncelleyen bir yasa tasarısı sunmuştur.
Hilton Hotel & Resorts: Müşteri ve kredi kartı veritabanı	Bazı satış notkası sistemlerinde kötücül yazılım bulunduğunu belirten bir sızma olayı yaşanmıştır. Çalınan verilerin; kart sahibi isimlerini, ödeme kartı numaralarını, güvenlik kodlarını ve son kullanma tarihlerini içerdiği kabul edilmiştir.	Olay sonrası ödeme kartı bilgilerini hedef alan yetkilendirilmemiş kötücül yazılımı tespit edip ortadan kaldırmak ve sistemlerin güvenliğini güçlendirmek için birtakım önlemler alınmıştır.

Tablo 2.1 Yakın geçmişte yaşanmış bazı veri ihlalleri (devamı)

U.S. Office of Personnel Management: ABD Federal Hükümetinin bir birimi	Haziran 2015'te yaklaşık 22 milyon insanı etkileyen bir veri ihlalinin hedefi olunduğu duyurulmuştur.	Veri ihlali, uzun yıllar sürebilecek büyük çapta karşı istihbarat tehdidi yaratmıştır.
Excellus BlueCross BlueShield: Müşteri veritabanı	Aralık 2013'te BT sistemlerinin ihlal edilmesiyle birlikte başlayan 10 milyondan fazla üyenin kişisel verileri açığa çıkmıştır.	Şirketin, aleyhine açılan davada müşterilerinin hassas verilerini korumak için gerekli yasal yükümlülüklerini yerine getirmekte başarısız olduğu öne sürülmüştür.

Veri güvenliğinin temel unsurları gizlilik, bütünlük ve kullanılabilirliktir. Veri güvenliği, kamu kurum ve kuruluşlarının hassas verilerini yetkisiz erişime ve veri hırsızlığına karşı korumaları için bir güvenlik modeli sunar. İhlalleri önlemek, riski azaltmak ve korumaları sürdürebilmek için kullanılan farklı veri güvenliği teknolojileri şunlardır [45]: "Veri Denetimi", "Gerçek Zamanlı Veri Uyarıları", "Veri Risk Değerlendirmesi", "Veri Minimizasyonu", "Eski Verilerin Temizlenmesi" ve "Veri Esnekliği".

- ***Veri Denetimi:*** Bir güvenlik ihlalinin temel nedenini araştırmaktır. Örneğin, erişim kontrolündeki değişikliklerin izlenmesi, hassas verilere ne zaman erişildiğinin tespit edilmesi, vb.
- ***Gerçek Zamanlı Veri Uyarıları:*** Veri etkinliklerini ve şüpheli olarak gözlemlenen davranışları gerçek zamanlı olarak izler. Kişisel verilerin kazaen imha edilmesi, kaybı, değişikliği veya yetkisiz ifşası durumlarının daha hızlı keşfedilmesini sağlar.
- ***Veri Risk Değerlendirmesi:*** Şirketlerin, hassas verilerini tespit etmelerine olanak tanır. Güvenlik açısından önem arz eden riskleri ön planda tutmak ve bu riskleri ortadan kaldırmak için güvenilir adımlar sunur. Süreç, küresel gruplar aracılığıyla erişilen hassas verilerin, eski verilerin ve / veya tutarsız izinlerin tanımlanmasıyla başlar. Risk değerlendirmeleri önemli bulguları

saptar ve güvenlik açıklarını tespit eder. İlave olarak her bir güvenlik açığının ayrıntılı analizlerini yapar ve öncelikli olanların düzeltilmesi yönünde öneriler içerir.

- ***Veri Minimizasyonu:*** Kuruluşların bireylerden topladıkları kişisel verileri sınırlandırmak ve yalnızca belirli iş amaçlarını gerçekleştirmek için ilgili veya gerekli bilgileri işlemek amacıyla gerçekleştirdiği önlemleri ifade eder. Örneğin bir Türkiye Cumhuriyeti kimlik numarasının ilk 7 rakamı bir veri tabanı içinde maskelenebilir.
- ***Eski Verilerin Temizlenmesi:*** Veri minimizasyon metodolojisinin temel bir bileşenidir. Erişilen bilgilerin gerçekten değerli olduğundan ve bir güvenlik tehdidi oluşturmadığından emin olmak için sürekli olarak eski verilerin temizlenmesi gerekir.
- ***Veri Esnekliği:*** Verilerin yedek kopyalarını oluşturarak, yanlışlıkla silinmesi veya bozulması veya bir veri ihlali sırasında çalınması durumunda verilerin kurtarılabilir olması durumudur.

Veri güvenliği, kuruluşların işlediği, muhafaza ettiği, aldığı ve ilettiği tüm verileri korumayı amaçlar. Verilerin, nasıl oluşturulduğu ve yönetildiği, nerede depolandığı ve tüm bu işlevler için hangi ürün ve hizmetlerin kullanıldığı önemli değildir, çünkü önemli olan şey verinin korunmasıdır. Veri ihlalleri, bir kuruluşun itibarına zarar verilmesinin yanı sıra, birtakım yasal süreçlerin başlanmasına ve büyük para cezalarına da neden olabilir. Verileri olası tehditlerden korumanın ve bu tehditlerle başa çıkmanın önemi her geçen gün daha fazla anlaşılmaktadır.

2.3 Kötücül Yazılımlar, Riskler, Tehditler ve Güvenlik Açıkları

Bir bilgi sisteminde güvenlik açığı, bir sistem veya ağda hasara neden olabilecek veya bir saldırganın sistemi bir şekilde manipüle etmesine izin verebilecek birtakım kusurların veya zayıflıkların mevcut olması şeklinde ifade edilir [46]. Bir bilgi sisteminde güvenlik açığından yararlanma şekli, güvenlik açığının niteliğine ve saldırganın nedenlerine bağlı olarak değişir. Güvenlik açıkları, çeşitli uygulamaların, sistem modüllerinin veya bir yazılım programındaki temel kusurların beklenmedik bir şekilde etkileşimleri sonucu ortaya çıkabilir. Bu

bölümde yaygın olarak karşılaşılan birkaç kötücül yazılımlar, güvenlik açıkları ve tehditlerinden bahsedilecektir.

2.3.1 Kötücül Yazılımlar

Her zaman yeni kötü amaçlı yazılımlar oluşturulmaktadır. Güncel kötü amaçlı yazılımların birçoğu, antivirus programları tarafından tanınmayacak şekilde değiştirilmiş yeni yapılarıyla ortaya çıkar ve bunlar genellikle eski kötü amaçlı yazılım programlarından türetilmiştir. Ancak yıllar boyunca, her biri hedefteki sistemleri farklı bir şekilde etkileyen birçok farklı türde kötü amaçlı yazılımlar oluşturuldu [47]: "Fidye Yazılımı (Ransomware)", "Virüsler (Viruses)", "Truva Atları (Trojans)", "Solucanlar (Worms)", vd.

- ***Fidye Yazılımı:*** Bu yazılım, veri depolama sürücülerini şifreleyerek sahibinin veri depolama alanlarına erişememesini sağlar. Şifreleme anahtarı karşılığında ödeme talep eden bir ültimatom verir. Fidye talebi karşılanmazsa, anahtar silinir ve veriler sonsuza dek kaybolur.
- ***Virüsler:*** Bir bilgisayar virüsü, kendisinin bir kopyasını oluşturarak başka bir programa ekler ve programın bir parçası haline gelerek yayılır. Virüs, yayılarak kendini çoğaltabilecek yeni alanlar bulur ve yayılırken de enfeksiyonlar bırakır. Hemen hemen tüm virüsler yürütülebilir bir dosyaya eklenir. Yani bir kullanıcı, virüsün enjekte olduğu ana bilgisayar dosyasını veya programını çalıştırana veya açana kadar virus etkin olmaz veya yayılmaz.
- ***Truva Atları:*** Truva atı, kurbanlarının sistemlerine yüklemeleri için tasarlanmış ve yasal bir program gibi görünen herhangi bir kötü amaçlı yazılım parçasıdır. Siber hırsızlar ve bilgisayar korsanları hedefledikleri sistemlere erişmek ve ele geçirmek için truva atını kullanabilirler. Kurbanlar genel olarak bir tür sosyal mühendislik aracılığıyla sistemlerine truva atları yükleme ve çalıştırma konusunda kandırılır. Truva atları enjekte olduğu sistemlere çok fazla zarar verebilir, çünkü etkinleştirildikten sonra siber suçluların kurbanını gözetlemesini, hassas verilerini çalmasını ve sistemine arka kapıdan erişim yapmasını sağlayabilir.

- ***Solucanlar:*** Solucanlar, kendi kendini kopyalayabilen ve e-postalar, SMS'ler gibi basit yollarla yayılabilen bir kötü amaçlı yazılım programlarıdır. Solucanlar, yayılmak için ya hedef bir sistemin güvenlik açıklarından faydalanırlar ya da kullanıcılara güvenli bir kaynaktan geliyormuş izlenimi yaratarak onları çalıştırmaları yönünde ikna etmek suretiyle bir tür sosyal mühendislik kullanırlar. Bir solucan, sistemdeki bir güvenlik açığı yoluyla bir bilgisayara girer ve sistemdeki dosya taşıma veya bilgi taşıma özelliklerinden yararlanarak yardımsız hareket etmesine olanak tanır.

Çoğu kötü amaçlı yazılım programının amacı hassas verilere erişmek ve bunları kopyalamaktır. Bazı ileri derecede gelişmiş kötü amaçlı yazılımlar, verileri özerk olarak kopyalayabilirler ve ardından bu verileri bir saldırganın gizlice bilgi çalmak için kullanabileceği bir bağlantı noktasına veya sunucuya gönderebilirler [48].

2.3.2 Riskler, Tehditler ve Güvenlik Açıkları

Veri güvenliği sorunlarını güçlü bir şekilde ele almak için, üç temel bileşen arasındaki ilişkiyi anlamak gerekir: tehdit, güvenlik açığı ve risk. Bu teknik terimler çok sık karıştırılabilmekte ve birbirinin yerine kullanılabilmektedir. Oysa bu üç temel bileşen, farklı anlamlara ve sonuçlara sahip farklı terimlerdir. Tehdit bir sisteme zarar verme potansiyeline sahip yeni bir olaydır. Güvenlik açığı, bilgisayar korsanlarının yararlanabileceği bir varlığın bilinen bir zayıflığıdır. Risk ise, bir güvenlik açığından faydalanan riskin ortaya çıkarabileceği kaybın veya hasarın potansiyel gücü olarak ifade edilir [49]. Şekil 2.4'te her üç temel bileşen arasındaki ilişki gösterilmiştir.

Şekil 2.4 Tehdit, güvenlik açığı ve risk bileşenleri arasındaki ilişki

a) Tehditler

Tehdit, bir sisteme veya genel olarak bir kuruluşa zarar verme potansiyeline sahip olan yeni veya keşfedilen bir olay olarak tanımlanır. Üç temel tehdit türü vardır [50]:

1) Seller, hortum, kasırgalar, depremler, çığ gibi doğal tehdit unsurları.
2) Bir çalışanın kazaen hassas bilgilere erişmesi veya yok etmesi veya değiştirmesi gibi kasıtlı olmayan tehditler.
3) Casus yazılımlar, kötü amaçlı yazılımlar veya kötü niyetli bir çalışanın eylemleri gibi kasıtlı olan tehditler.

Solucanlar ve virüsler tehdit olarak sınıflandırılır, çünkü insanlar tarafından işlenenlerin aksine otomatik bir saldırıya maruz kalarak kuruluşlara zarar verebilirler [50]. Öte yandan, verileri yok etmeyi ve operasyonları aksatmayı amaçlayan tehdit aktörleri, kuruluşların ilk önce savunmaya çalıştıkları başlıca korkulardan ikisidir. Güvenlik programları, her türlü tehdit senaryolarına karşı savunmak ve güvenlik tehditlerini ele almak için özel olarak oluşturulmuştur. Olası tehditlere iyi bir örnek, kötü amaçlı yazılım, fidye yazılımı ve virüsleri verebiliriz.

Bazı tehditler kontrol edilemeyebilir ve genellikle önceden tespit edilmesi zor veya imkansız olabilir. Yine de, belirli önlemler tehditlerin düzenli olarak değerlendirilmesine yardımcı olur, böylece bir durum meydana geldiğinde daha hazırlıklı olunur [50, 51]. Örneğin, güvenlik açıklarını keşfetmek için gerçek dünyadaki tehditleri modelleyerek sızma testleri yapmak, bir sistemi belirli bir tehdide karşı korumak için en iyi yaklaşımları belirlemek, farklı tehdit türlerini değerlendirmek için düzenli tehdit değerlendirmeleri gerçekleştirmek ve yeni tehditlerin hızla belirlenebilmesi için siber güvenlikle ilgili güncel eğilimlerden haberdar olmak gibi.

b) Güvenlik Açıkları

Güvenlik açığı, bir veya daha fazla saldırgan tarafından istismar edilebilen bir varlığın (kaynağın) bilinen bir zayıflığını ifade eder. Başka bir deyişle, bir saldırının başarılı olmasına imkan veren bilinen bir sorun olarak ifade edilir [50, 52]. Örneğin, işletmeden bir çalışan ayrıldığında ve kurumsal tüm hesaplarına

erişiminin engellenmesi ve tüm yetkilerinin kaldırılması unutulduğunda, bu durum işletmeyi hem kasıtlı hem de kasıtsız tehditlere karşı savunmasız hale getirebilir.

Güvenlik açıklarını sürekli gözlemlemek ve sistemi belirli aralıklarla test etmek gerekir, çünkü sistemlerin güvenliğinin sürekli olarak sağlanması önemlidir. Sistemin zayıf noktaları belirlenerek, hızlı yanıt için bir strateji geliştirilebilinir. Güvenlik açıkları tespit edilirken genellikle sorulması gereken bazı sorular vardır, bu sorular [52]:

- Veriler saha dışında güvenli bir yerde yedekleniyor ve saklanıyor mu?
- Veriler bulutta mı depolanıyor? Şayet bulutta depolanıyorsa, veriler bulut güvenlik açıklarından tam olarak nasıl korunuyor?
- Bilgilere kimlerin erişebileceğini, kimlerin değiştirebileceğini veya silebileceğini belirlemek için ne tür bir ağ güvenliğine sahipsin?
- Ne tür bir antivirüs programı kullanılıyor? Lisanslar güncel mi? Gerektiği kadar sık test ediliyor mu?
- Olası bir güvenlik açığından yararlanılması durumunda bir veri kurtarma planı var mı?

Güvenlik açığı terimi, donanım ve yazılımdaki potansiyel zayıf noktaları ortaya çıkarır. Uygulamalarda, zayıflıktan yararlanılmasını sağlamlaştırmak ve önlemek için güvenlik açığı genellikle üretici tarafından yamalanabilir. Yetkisiz erişim, bir güvenlik açığından yararlanan birine örnek olabilir. Sistem yalnızca yetkili erişime izin vermelidir ve yetkisiz birine erişim izni verilirse, BT güvenliğini ihlal eder ve erişim kontrollerini atlar [52]. Güvenlik açıklarını anlamak, riski yönetmenin ilk adımıdır.

Birçok güvenlik açığı nedeni vardır [52, 53]: karmaşıklık, aşinalık, bağlantı, kötü parola yönetimi, işletim sistemi kusurları, internet kullanımı, yazılım hataları, kontrol edilmemiş kullanıcı girişi, insan.

- ***Karmaşıklık:*** Karmaşık sistemler, bir kusur, yanlış yapılandırma veya istenmeyen erişim olasılığını artırır.

- ***Aşinalık:*** Ortak kod, yazılım, işletim sistemleri ve donanım, bir saldırganın bilinen güvenlik açıklarını bulması veya bunlarla ilgili bilgilere sahip olma olasılığını artırır.
- ***Bağlantı:*** Bir cihaza çok fazla bağlantı yapılması güvenlik açığı riskini artırır, yani ne kadar çok bağlantı trafiği oluşursa o derece güvenlik açığı olasılığı yüksek olur.
- ***Kötü parola yönetimi:*** Zayıf parolalar kaba kuvvet saldırısı ile kolayca kırılabilir. Özellikle aynı parolaların kullanılması ve düzenli aralıklarla parolaların değiştirilmemesi bir veli ihlaline neden olabilir.
- ***İşletim sistemi kusurları:*** Herhangi bir yazılımda olduğu gibi, işletim sistemlerinde de kusurlar olabilir. Varsayılan olarak güvenli olmayan ve tüm kullanıcılara tam erişim sağlayan işletim sistemleri, virüslerin ve kötü amaçlı yazılımların komut yürütmesine izin verebilir.
- ***İnternet kullanımı:*** İnternet, bilgisayarlara otomatik olarak yüklenebilen casus yazılım ve reklam yazılımlarıyla doludur.
- ***Yazılım hataları:*** Programcılar, yanlışlıkla veya kasıtlı olarak yazılımda yararlanılabilir bir hata bırakabilir.
- ***Kontrol edilmemiş kullanıcı girişi:*** Tüm girdilerin güvenli olduğunun varsayılması halinde, bir web site veya yazılım istenmeyen SQL komutlarını çalıştırabilir.
- ***Insan:*** Bir organizasyonda en büyük güvenlik açığı, sistemin sonunda yer alan "insan" olarak ifade edilir. Nitekim sosyal mühendislik, kuruluşların çoğunluğu için en büyük tehdit unsurudur.

Güvenlik açığı yönetimi, güvenlik açıklarını tanımlama, sınıflandırma, düzeltme ve azaltmaya yönelik döngüsel bir uygulamadır. Güvenlik açığı yönetiminin temel unsurları şunlardır: güvenlik açığı algılama, güvenlik açığı değerlendirme ve güvenlik açığını düzeltme. Bir güvenlik açığı bulunduğunda, güvenlik açığı değerlendirme sürecinden geçer [53]:

- ***Güvenlik açıklarını belirleme:*** Bir siber saldırının bir güvenlik açığından yararlanabileceğini düşündüren anormallikleri bulmak için ağ taramalarını,

kalem testi sonuçlarını, güvenlik duvarı günlüklerini ve güvenlik açığı tarama sonuçlarını analiz etme.

- ***Güvenlik açıklarını doğrulama:*** Tanımlanan güvenlik açığından yararlanılıp yararlanılamayacağına karar verilmesi ve risk düzeyini anlamak için istismarın şiddetinin sınıflandırılması.
- ***Güvenlik açıklarını azaltma:*** Bir yamanın mevcut olmaması durumunda karşı önlemlere ve bunların etkinliğinin nasıl ölçüleceğine karar verilmesi.
- ***Güvenlik açıklarını giderme:*** Etkilenen yazılım veya donanımı mümkün olduğunca güncellenmesi.

Güvenlik açığı tespit yöntemleri şunlardır [53, 54]: güvenlik açığı taraması, penetrasyon testi ve Google korsanlığı.

- ***Güvenlik açığı taraması:*** Güvenlik açığı tarayıcısı, bilgisayarları, ağları veya uygulamaları bilinen güvenlik açıklarına karşı değerlendirmek için tasarlanmış bir yazılımdır. Bir ağ içindeki yanlış yapılandırmadan ve hatalı programlamadan kaynaklanan güvenlik açıklarını belirleyip tespit edebilir ve kimliği doğrulanmış ve doğrulanmamış taramalar gerçekleştirebilir.
- ***Penetrasyon testi:*** Kalem testi veya etik hack olarak da bilinen penetrasyon testi, bir saldırganın yararlanabileceği güvenlik açıklarını bulmak için bir bilgi teknolojisi varlığını test etme uygulamasıdır. Penetrasyon testi yazılımla otomatik hale getirilebilir veya manuel olarak gerçekleştirilebilir.
- ***Google korsanlığı:*** Güvenlik açıklarını bulmak için Google veya Microsoft'un Bing uygulamaları gibi bir arama motorunun kullanılmasıdır. Google korsanlığı, bulut hizmetlerinin yanlış yapılandırılması nedeniyle yanlışlıkla açığa çıkan veya bulunması zor bilgileri bulan sorgularda gelişmiş arama operatörlerinin kullanılmasıyla gerçekleştirilir. Güvenlik araştırmacıları ve saldırganlar, halka açık olması amaçlanmayan hassas bilgileri bulmak için bu hedeflenen sorguları kullanır.

Güvenlik açıkları altı geniş kategoride değerlendirilir [53, 54]:

1) **Donanım:** Neme, toza, kirlenmeye, doğal afete, zayıf şifrelemeye veya ürün yazılımı açıklarına karşı duyarlılık.

2) **Yazılım:** Yetersiz test, denetim izi eksikliği, tasarım kusurları, bellek güvenliği ihlalleri (arabellek taşmaları, aşırı okumalar, sarkan işaretçiler), giriş doğrulama hataları (kod enjeksiyonu, siteler arası komut dosyası oluşturma (XSS), dizin geçişi, e-posta enjeksiyonu, HTTP üstbilgisi enjeksiyonu, HTTP yanıt bölme, SQL enjeksiyonu), kullanıcı arayüzü hataları, vd.
3) **Ağ:** Korunmayan iletişim hatları, ortadaki adam saldırıları, güvenli olmayan ağ mimarisi, kimlik doğrulama eksikliği veya varsayılan kimlik doğrulama.
4) **Personel:** Zayıf işe alım politikası, güvenlik bilinci ve eğitim eksikliği, güvenlik eğitimine yetersiz bağlılık, zayıf parola yönetimi veya e-posta ekleri aracılığıyla kötü amaçlı yazılım indirme.
5) **Fiziksel site:** Doğal afete maruz kalan alan, güvenilmez güç kaynağı veya anahtar kart erişimi olmayan alan.
6) **Örgütsel:** Denetim eksikliği, süreklilik planı, güvenlik veya olay müdahale planı.

c) Riskler

Risk, bir güvenlik açığından faydalanan riskin ortaya çıkarabileceği potansiyel kayıp veya hasar olarak ifade edilir. Risk örnekleri arasında finansal kayıplar, mahremiyet kaybı, itibarın zarar görmesi, yasal çıkarımlar ve hatta can kaybı yer alır [55].

Ayrıca, risk şu şekilde formülize edilir:

$$Risk = Tehdit \quad X \quad Güvenlik\ Açığı$$

Riskin potansiyel gücünü azaltmak için bir risk yönetim planının oluşturulması ve uygulanması gerekir. Risk yönetiminde strateji geliştirilirken dikkate alınması gereken bazı temel konular vardır [55]:

- ***Riski değerlendirme ve ihtiyaçları belirleme:*** Bir risk değerlendirme çerçevesi tasarlama ve uygulaması söz konusu olduğunda, ele alınması gereken en önemli şey ihlallere öncelik verilmesidir. Her kuruluşta sıklık farklılık gösterse de, bu düzeydeki değerlendirme düzenli ve tekrar eden bir temelde yapılmalıdır.

- ***Tam bir paydaş perspektifi dahil etme:*** Paydaşlar, kuruluş sahiplerinin yanı sıra çalışanları, müşterileri ve hatta satıcıları içerir. Tüm bu oyuncular, organizasyonu olumsuz yönde etkileme potansiyeline (potansiyel tehditler) sahiptir, ancak aynı zamanda riski azaltmaya yardımcı olacak varlıklar olabilirler.
- Risk yönetiminden sorumlu merkezi bir çalışan grubunun ve bu faaliyet için uygun finansman düzeyinin belirlenmesi gerekir.
- Uygun politikaların ve ilgili kontrollerin uygulanması ve uygun son kullanıcıların tüm değişikliklerden haberdar edilmesi gerekir.
- ***Politika ve kontrol etkinliğinin izlenmesi ve değerlendirilmesi:*** Risk kaynakları sürekli değiştiğinden, risk değerlendirme ekibinin risk değerlendirme çerçevesinde gerekli düzenlemeleri yapmaya hazırlıklı olması gerekir. Bu durum, değişime uygun olarak yeni izleme araçlarının ve tekniklerinin dahil edilmesini de içerebilir.

Sonuç olarak; risk, bir organizasyon içindeki sistemlerle ve sistemlerin kullanımıyla ilgili olası zararı temsil eder. Tehdit, güvenlik açıkları ve riskler farklıdır ve siber güvenlik söz konusu olduğunda genellikle birbiriyle bağlantılıdır [54, 55]. Bu üç güvenlik bileşeninin tanımlarını doğru bir şekilde anlamak oldukça önemlidir, çünkü riski azaltmak için olası tehditleri belirlemek, güvenlik açıklarını tespit etmek ve ele alıp değerlendirmek için tasarlanacak çerçevenin daha etkili olmasını sağlayacaktır.

2.4 Güvenlik Denetimi

Güvenlik denetimi, kuruluşların siber güvenlik de dahil olmak üzere genel güvenlik duruşlarını test edip değerlendirebilecekleri birçok yöntemin üst düzey açıklamasıdır [56]. İstenilen sonuçları elde etmek ve iş hedeflerini karşılamak için birden fazla türde güvenlik denetimi uygulamak gerekebilir. Düzenli denetimler, yeni güvenlik açıklarını ve organizasyonel değişimin istenmeyen sonuçlarını yakalayabilir ve bunun da ötesinde, bazı endüstriler için (özellikle tıbbi ve finans) kanunen zorunludur.

Bir siber güvenlik denetimi beş adımdan oluşur [53, 54, 55, 56]: hedefleri tanımlama, denetimi planlama, denetim işini gerçekleştirme, sonuçları raporlama, gerekli işlemi yapma.

1) **Hedefleri tanımlama:** Denetim ekibi, güvenlik denetimini yaparak ulaşmayı amaçladığı hedefleri belirlemesidir.
2) **Denetimi planlama:** İyi düşünülmüş ve iyi organize edilmiş bir plan, güvenlik denetiminde başarı için çok önemlidir. Denetim görevlerini yerine getirmek için atanan yönetim ekibinin ve BT sistem yöneticilerinin rollerini ve sorumluluklarını, ayrıca sürecin zamanlamasını ve metodolojisini tanımlamak gerekir. Tüm ayrıntılara karar verdikten sonra, denetim başlamadan önce tüm personelin süreç hakkında ortak bir anlayışa sahip olmasını sağlamak için planın belgelenmesi ve dağıtılması önemli bir husustur.
3) **Denetim işini gerçekleştirme:** Denetim ekibi, denetimi planlama aşamasında üzerinde mutabık kalınan plan ve metodolojilere göre hareket etmelidir. Ağ güvenliğini, veri erişim düzeylerini, kullanıcı erişim haklarını ve diğer sistem yapılandırmalarını değerlendirmek için BT kaynaklarında tarama yapılır. Bu süreç sırasında, güvenlik kaygıları hakkındaki bilgileri ve şirket güvenlik politikasına bağlılıkları değerlendirmek için BT ekibinin dışında diğer çalışanlarla da görüşülmesi, böylece şirketin güvenlik prosedürlerindeki herhangi bir boşluluğun giderilmesi sağlanabilir.
4) **Sonuçları raporlama:** Rapor, sistemlerde tespit edilen tüm güvenlik risklerinin ve güvenlik açıklarının bir listesini ve ayrıca BT personelinin bunları azaltmak için gerçekleştirmesini önerdiği eylemleri içermelidir.
5) **Gerekli işlemi yapma:** Denetim raporunda ana hatları verilen önerilerin uygulanmasıdır. Örneğin, belirli bir güvenlik açığını veya zayıf noktayı düzeltmek için iyileştirme prosedürlerinin uygulanması, çalışanların veri güvenliği uyumluluğu ve güvenlik bilinci konusunda eğitilmesi, hassas verileri işlemek ve kötü amaçlı yazılım ve kimlik avı saldırılarının belirtilerini tanımlamak için ek olarak en iyi uygulamaların benimsenmesi, mevcut sistemleri güçlendirmek için yeni teknolojilerin edinilmesi ve güvenlik riski için altyapının düzenli olarak izlenmesi gibi.

Güvenlik denetiminin ve risk değerlendirmesinin her biri, kuruluşlar için güvenlik risklerini inceleme ve değerlendirme sürecini içerir. Aralarındaki farklar, zamanlamaları ve kapsamlarıyla ilgilidir. Risk değerlendirmesinin amacı, bilinen güvenlik risklerini göz önünde bulundurarak BT altyapısının en iyi şekilde nasıl inşa edileceğini belirlemektir. Dolayısıyla, bu faaliyet, dış faktörlere ve bunların altyapıyı nasıl etkilediğine odaklanır. Güvenlik denetimi ise, mevcut sistem ve operasyonların güvenliğini test etmek ve değerlendirmek için mevcut bir BT altyapısı üzerinde bir denetim gerçekleştirir [57].

Bir organizasyonda iki tür güvenlik denetimi vardır [57]: dış denetim ve iç denetim. Dış denetim, kamuya açık bilgilerin toplanmasını ve dışarıdan sızma durumunu kapsar. İç denetim, hassas bilgilerin toplanmasını, güvenlik politikasının gözden geçirilmesini, bilgi sistemi ve altyapısını, kişisel görüşmeyi ve fiziksel güvenliği içerir.

Güvenlik denetimlerinde sistemlerin ve ağların güvenlik seviyesini tespit etmek için aşağıda belirtilen standart teknikler kullanılır [57, 58]:

- ***Ağ Tarama:*** Ağ tarama aracı, ana bilgisayar ile kuruluş ağı arasındaki bağlantıyı doğrulamak için bağlantı noktasını tarar. Böylelikle tüm aktif ana bilgisayarların, yazıcıların, anahtarların ve yönlendiricilerin tam listesi sağlanır. İşletme, ağ taramasıyla yetkisiz ağ bağlantısını, savunmasız servisi doğrulayabilir ve adli kanıt toplayabilir.
- ***Güvenlik Açığı Taraması:*** Güvenlik açığı taraması, açık bağlantı noktalarını ve ilişkili güvenlik açığı verilerini ayırt eder. Ayrıca, tespit edilen güvenlik açıklarının azaltılmasına da rehberlik eder. Güvenlik açığı tarayıcısı, saldırganlar bulmadan önce güvenlik açıklarını bulmaya yardımcı olan etkin araçlar da sağlar. Ek olarak, kuruluş, kendi güvenlik düzeyini ve dış güvenlik açıklarına maruz kalma olasılığını kolayca ölçebilir. Dahası güvenlik açığı taraması, uygulamaları, işletim sistemini, yanlış yapılandırılmış ayarları, ağlardaki etkin ana bilgisayarları ve eski yazılım sürümlerini tanımlar.

- ***Şifre Kırma:*** Zayıf şifreleri bulmak ve şifre karmalarını almak için kullanılan şifre kırma yazılımıdır. Karmalar bulunduktan sonra, şifre kırıcı, doğru şifre eşleşene kadar karmalar üretir.
- ***Günlük İncelemesi:*** Günlüklerde güvenlik duvarı günlükleri, IDS günlükleri, sunucu günlükleri bulunur. Bu günlükler, tanımlanmış güvenlik politikası ile eşleştirilebilen devam eden etkinliklerin gerçek bir görüntüsünü verir. Günlük incelemeleri sonrası kuruluşlar, hassas sistem veya verilere erişimi kısıtlamak için mevcut güvenlik politikalarını değiştirebilir.
- ***Virüs Algılama:*** İşletmeler, dosyaların silinmesine, açılır ekran mesajına veya hassas bilgilerin yok edilmesine neden olan virüslere, solucanlara, kötü amaçlı yazılımlara eğilimlidir. Virüs tespit programı, ağ yapılarına ve e-posta sunucularına kurulabilir ve sistemlere enjekte olmuş mevcut virüsleri tanımlar. Virüsler, ağa girmeden önce tespit edilir, ayrıca e-postalarda, USB sürücüsünde, sabit diskte, belgelerde ve yerel ana bilgisayarda, web sitelerde virüsler tespit edilebilir. Virüslerden ve diğer kötü amaçlı yazılımlardan korunmak için kuruluşların lisanslı antivirüs programları kullanmaları ve düzenli olarak programları güncellemeleri gerekir.
- ***Sızma Testi:*** Sızma testi, sistem uygulamasına ve yapısına bağlı olarak sistemin güvenlik özelliklerinin atlatılması anlamına gelir. Bu tür testler, araçları ve teknikleri kullanarak sisteme erişim elde etme yöntemini tanımlar. Sızma testi çalıştırılırken ağ yanıt süresi yavaş olabilir. IP adresleri, kısıtlanmış ana bilgisayarlar, test teknikleri, test süresi, temas noktaları gibi birkaç ayrıntıyı test ederken göz önünde bulundurmak gerekir.

Sonuç olarak güvenlik yapısı ayrıca organizasyon altyapısına da bağlıdır. Bu nedenle, güvenlik denetimi tek yönlü bir iş değildir, aksine süreklilik isteyen ve bir süreç gerektiren kapsamlı bir iştir. Denetim, kuruluşun güvenlik politikasının etkinliğini inceler ve değerlendirir [58]. Güvenlik denetimi, denetim sürecinde bulunan eksiklikleri düzeltir ve politikayı iyileştirir.

3
ERİŞİM DENETİMLERİ

Erişim denetimi, kullanıcıların söyledikleri kişi olduklarını ve şirket verilerine uygun erişime sahip olduklarını garanti etmenin bir yöntemidir. İleri düzey erişim kontrolünde, verilere erişimin seçici bir şekilde kısıtlanması söz konusudur ve iki ana bileşenden oluşur [59]: kimlik doğrulama ve yetkilendirme. Kimlik doğrulama, birinin iddia ettiği kişi olduğunu doğrulamak için kullanılan bir tekniktir. Veri güvenliğini sağlamada kimlik doğrulama yöntemi tek başına yeterli değildir. Bir kullanıcının verilere erişmesine veya denemek istediği işlemi yapmasına izin verilip verilmeyeceğini belirleyen ek bir yetki tanımlamasına ihtiyaç vardır. Esasen, bu güvenlik unsuru bilgi akışını düzenler ve bir kullanıcının ve bir sistemin diğer sistemler veya kaynaklarla nasıl bağlantı kurabileceğini veya etkileşime girebileceğini belirler [60].

Erişim denetimi, kullanıcı adları (ID'leri) ve şifreleri, PIN'ler, biyometrik taramalar ve güvenlik belirteçlerini içerebilen çeşitli oturum açma kimlik bilgilerini doğrulayarak kullanıcıları tanımlar. Çoğu erişim denetimi sistemi, kullanıcıların kimliğini doğrulamak için birden çok kimlik doğrulama yöntemi gerektiren bir yöntem olan çok faktörlü kimlik doğrulama tekniğini tercih eder [38]. Kimlik doğrulama aşamasından sonra gelen erişim denetimi yöntemi, uygun erişim düzeyini tanımlar ve kullanıcıların kimlik bilgileri ve IP adresleri ile ilişkili olarak izin verilen eylemleri yetkilendirir.

Erişim denetimi, oldukça önemli bir yöntemdir, çünkü erişim denetimi olmadan veri güvenliği olmaz [44, 45, 61]. Erişim denetimi, kurumsal verilerin, kişisel olarak tanımlanabilir bilgilerin ve fikri mülkiyet dahil olmak üzere tüm gizli ve hassas bilgilerin yanlış kişilerin eline geçmesini önler. Sağlam bir erişim denetimi politikası olmazsa eğer, kuruluşlar hem iç hem de dış kaynaklardan veri sızıntısı riskine maruz kalabilir. Erişim denetimi, kaynakların, uygulamaların ve verilerin hem şirket içinde hem de bulutta yer aldığı karma (hibrit) ve çoklu bulut

ortamlarına sahip kuruluşlar için özellikle önemlidir. Çünkü erişim denetimi, bu ortamlara "tek oturum açma" dışında daha sağlam erişim güvenliği sağlayabilir [62].

3.1 Erişim Denetimi Türleri

İki ana erişim denetimi türü vardır: fiziksel ve mantıksal erişim denetimi. Fiziksel erişim denetimi binalara, odalara, alanlara ve BT varlıklarına erişimi sınırlarken, mantıksal erişim denetimi bilgisayar ağlarına, sistem dosyalarına ve verilere olan bağlantıları sınırlar [63].

3.1.1 Mantıksal Erişim Denetimi

Mantıksal erişim denetimi, kimlik doğrulama ve yetkilendirme süreçlerini kapsar ve bu yönüyle fiziksel erişim denetiminden farklıdır. Fiziksel erişim denetimi, anahtarlar ve rozetler kullanır. Mantıksal erişim denetimleri, gelişmiş şifre programları ve gelişmiş biyometrik güvenlik özellikleri kullanır. Bu özellikler kullanıcıları / çalışanları tanımlar. Sistem kullanıcının verilere erişimi için uygun bir yetkiye sahip olup olmadığını belirler [63].

Mantıksal erişim denetiminin birçok avantajı vardır. Ana faydası, daha yönetilebilir ve kolay uygulanabilir teknikler içermesidir. Örneğin, bir işverenin bir çalışanın yetkisini derhal iptal edebilir veya değiştirebilir. Ayrıca bir işveren, rozetin fiziksel kontrolünü ele geçirmeden çalışanın rozet erişimini devre dışı bırakabilir.

Bilgisayarlara, telefonlara ve web sitelere ve çevrimiçi hizmetlere erişmek için kullanılan şifreler, mantıksal erişim kontrolünün örnekleridir [60, 63]. Doğru kullanıcı adı ve parola kombinasyonu, bir kuruluş içindeki kullanıcı, çalışan veya müşterinin belirli işlevler için erişim izinlerini doğrular. Bu kimlik doğrulama türü sayısı giderek artan mantıksal erişim kontrollerinden yalnızca biridir.

3.1.2 Fiziksel Erişim Denetimi

Basit bir tabirle fiziksel erişim denetimi, fiziksel bir alana erişimin sınırlandırılması şeklinde tanımlanabilir. Bu tür erişim denetimi, odalara, binalara ve fiziksel BT varlıklarına erişimi kısıtlar. Ayrıca, fiziksel erişim denetimi, kısıtlı alanlara geçişin kontrolünü yapar ve alanlara kimin girip çıktığını takip eder. Fiziksel erişim

denetimi örnekleri arasında anahtarlıklar, biyometri (parmak izi, ses, yüz, iris, el yazısı ve kişileri tanımak için kullanılan diğer otomatik yöntemleri içerir) ve kapı erişim sistemlerinde şifreli kilitler bulunur [60, 63].

3.2 Güvenlik Seviyesi ve Genel Erişim İlkeleri

3.2.1 Güvenlik Seviyesi

Kullanıcılar ve nesneler, farklı güven ve duyarlılık düzeylerine göre sınıflandırılır. Bu seviyeler, iyi bilinen güvenlik sınıflandırmalarını temsil eder [63, 64]: ***çok gizli*** – ***gizli*** – ***özel*** – ***kısıtlı***.

İzin düzeyi, güvenlik iznine sahip bir kişiye veya gizli bilgileri işleyen bir bilgisayara veya sınıflandırılmış bilgileri depolamak için fiziksel olarak güvenlik altına alınmış bir alana verilen güven düzeyini gösterir. Seviye, kişi, cihaz veya konum tarafından saklanacak veya işlenecek en yüksek sınıflandırılmış bilgi seviyesini gösterir. Sınıflandırma seviyesi ise, bir belgedeki veya bir bilgisayar dosyasındaki gibi bazı bilgilerle ilişkili hassasiyet düzeyini gösterir. Güvenlik seviyesi, bir izin seviyesi veya bir sınıflandırma seviyesi için genel bir terimdir [64].

3.2.2 Erişim, En Az Ayrıcalık ve Görevler Ayrılığı İlkeleri

Bilinmesi gereken genel erişim ilkeleri şunlardır [63, 64]:

- Yalnızca güvenli bölgeye sürekli erişim gereksinimi olan operatörlerin (kullanıcılar ve yöneticiler) güvenli bölge içinde hesap sahibi olmasına izin verilir.
- Ayrıcalıklar yalnızca doğrulanmış bir kullanıcıya atanır. Diğer sistem işlevlerine erişim devre dışı bırakılır.

En az ayrıcalık ilkeleri şunlardır [63, 64]:

- Kullanıcı ve yönetici ayrıcalıkları, tüm ayrıcalıkların bireysel ihtiyaçlara göre özelleştirilmesine izin verecek şekilde kontrol edilir.
- Hesaplara ihtiyaca göre belirlenmiş özel ayrıcalıklar verilir. Ek ayrıcalıklar ise yalnızca anlık ihtiyacı karşılamak ve işin sekteye uğramaması için geçici

olarak verilir. Bir çalışanın rollerini değiştirmesi veya organizasyondan ayrılması durumunda ayrıcalıklar derhal iptal edilir.

Görevler ayrılığı ilkeleri şunlardır [63, 64]:

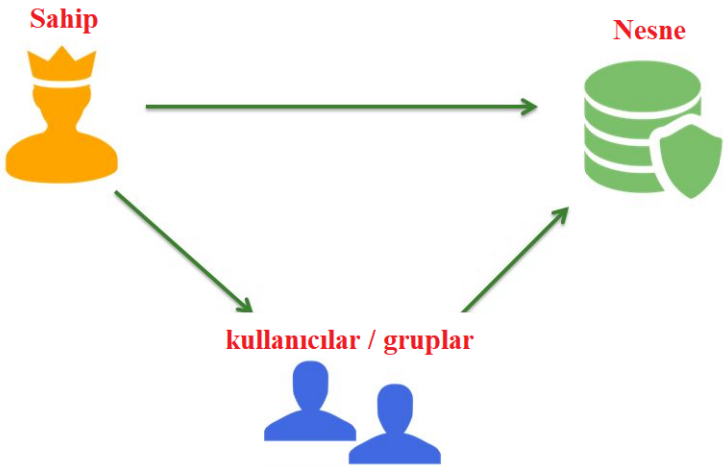
- İkili yetkilendirme ilkesinin etkinleştirilmesi gerekir (İkili yetkilendirme ilkesi, bir işlemi yetkilendirmek için iki ayrı kişi gerektiren bir denetimdir. İlk kişi talebi oluşturmaktan sorumludur (yapıcı olarak bilinir), ikinci kişi ise etkinliği kontrol eder ve onaylar (denetleyici olarak bilinir))
- Hassas görevler ayrılır. Yani bu durum, bazı rollerin aynı kişi tarafından temsil edilemeyeceği anlamına gelir, örneğin, uygulama yöneticisi ve güvenlik görevlisi, ağ yöneticisi ve işletim sistemi yöneticisi, işlem sunumu ve işlem onayı, veritabanı yöneticisi (tabloları ve prosedürleri oluşturan) ve veri kullanıcısı (verileri seçen, ekleyen, güncelleyen veya silen).

3.3 Erişim Denetimi Modelleri

Dört ana tip erişim denetimi modeli vardır. Kuruluşlar, kaynakların kullanabilirliğine, organizasyon yapısına ve gereksinimlerine göre en uygun yöntemi seçerler. Dört ana erişim denetimi modeli şunlardır [65]: Rol Tabanlı Erişim Denetimi, Öznitelik Tabanlı Erişim Denetimi, Zorunlu Erişim Denetimi ve İsteği Bağlı Erişim Denetimi.

3.3.1 İsteği Bağlı Erişim Denetimi

Bu erişim denetimi yöntemi, yetkili kullanıcılar tarafından belirlenen bir erişim ilkesi aracılığıyla erişim izni veren / kısıtlayan bir erişim denetimi türüdür ve genellikle "bilinmesi gereken" erişim modeli olarak adlandırılır [66]. Belirli kurallara göre erişim hakları atamanın bir yoludur. Başka bir deyişle, veri sahibi erişimi belirler. Şekil 3.1'de bir veri sahibinin başka kullanıcılara veya gruplara erişim izni verdiği gösterilmiştir.



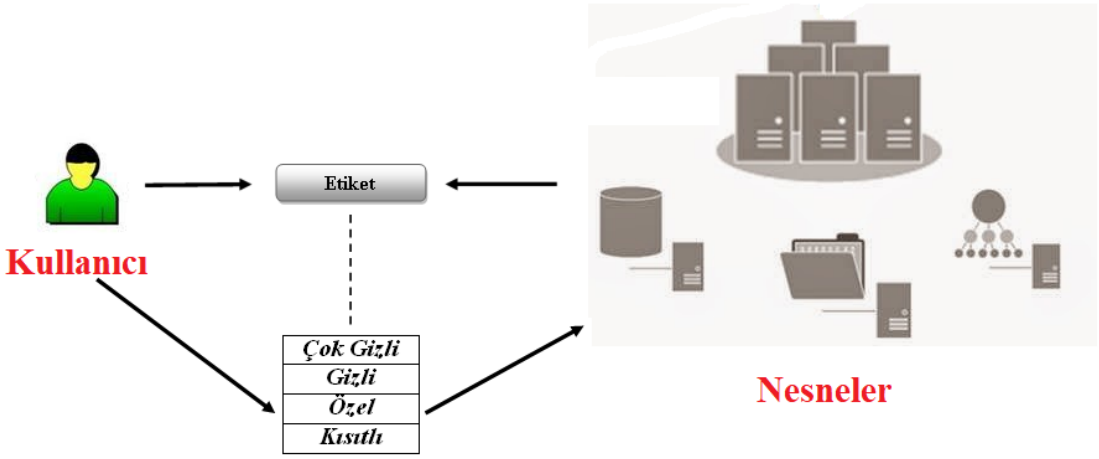
Şekil 3.1 İsteğe bağlı erişim denetimi modelinde erişim izni yapısı

Diğer erişim kontrol yöntemlerine kıyasla en az kısıtlayıcı model olan İsteğe Bağlı Erişim Denetimi, yetkili kişilere, sahip oldukları nesneler ve bu nesnelerle ilişkili programlar üzerinde tam kontrol yetkisi verir. Bu yöntem ile kullanıcılar, diğer kullanıcıların erişim türünü belirleyebilir ve nesne sahipliğini başka bir kullanıcıya aktarabilir. Linux'ta dosya izni, İsteğe Bağlı Erişim Denetiminin genel bir biçimidir [66, 67].

İsteğe bağlı erişim denetimi yalnızca, sahibinin şirket verilerini güvenli bir şekilde paylaşmaya istekli olmasıyla sınırlıdır. İsteğe bağlı erişim denetimi, BT personeli olmayan küçük işletmeler için genellikle iyi bir seçimdir, çünkü en az kısıtlayıcı erişim kontrol modeli olduğu için basitlik ve rahatlık sunar [67]. Açık bir ifadeyle bu model ile, az sayıdaki kullanıcının gün boyunca bilgi paylaşmasına izin verilerek, işletmenin sorunsuz bir şekilde işlemesine olanak tanınır.

3.3.2 Zorunlu Erişim Denetimi

Zorunlu erişim denetimi, hiyerarşik bir modele dayanmaktadır. Hiyerarşi, güvenlik düzeyine (çok gizli, gizli, özel, kısıtlı, vb.) bağlıdır. Tüm kullanıcılara bir güvenlik veya yetki seviyesi atanır. Tüm nesnelere bir güvenlik etiketi atanır. Kullanıcılar yalnızca hiyerarşide kendilerininkine eşit veya onlardan daha düşük bir güvenlik düzeyine karşılık gelen kaynaklara erişebilir (Şekil 3.2).



Şekil 3.2 Zorunlu erişim denetimi modelinin yapısı

Modelde, erişim yönetici tarafından kontrol edilir. Yönetici tüm izinleri belirler. Örneğin, kanunların vermiş olduğu yetki ile mahkemelerin kişilerin izni olmadan nüfus kütüklerine, iletişim bilgilerine, sürücü kayıtlarına ve diğer şahsi verilerine erişmesine izin vermektedir.

Modelde kullanıcılar, nesnenin sahibi olsalar bile kendi izinlerini ayarlayamazlar. Bu nedenle, bu modeli kullanan sistemler çok güvenli kabul edilir. Bunun nedeni merkezi yönetimdir. Merkezi yönetim, yöneticinin kimin neye erişimi olduğunu kontrol etmesini kolaylaştırır [68].

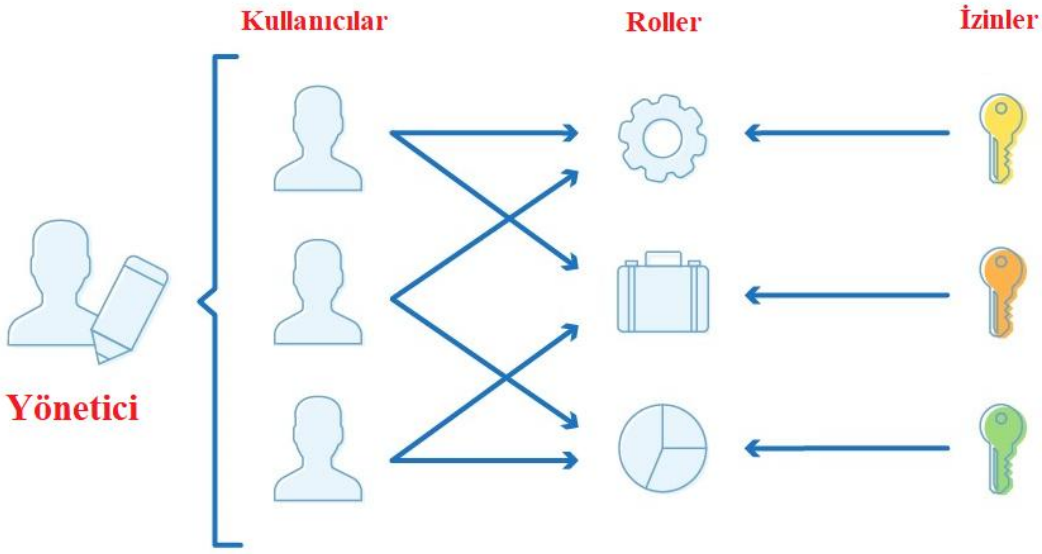
Bu modelin bazı dezavantajları vardır. Bu modeli kullanan sistemleri yönetmek oldukça zahmetli olabilir. Bunun nedeni, yöneticinin tüm izinleri ataması gerektiğidir. Bu nedenle yönetici, yapılandırma ve bakım için tüm yükü üstlenir. Sistemler büyüdükçe ve daha karmaşık hale geldikçe, bir yönetici çabucak bunalabilir. Bu, modelin genellikle İnternet tabanlı uygulamalarda kullanılmamasının ana nedenlerinden biridir. Zorunlu erişim kontrolü modeli, çoğunlukla önceliğin gizliliğe dayalı olduğu bir sistemde kullanılır [66, 67, 68].

3.3.3 Rol Tabanlı Erişim Denetimi

Rol tabanlı erişim denetimi (RBAC), sisteme erişimi kontrollü bir şekilde sınırlandıran bir mekanizmadır. Yetkilendirilmiş kullanıcılara erişim izni vermek için izin ve ayrıcalıkların tanımlanmasını içerir. Birçok büyük kuruluş, çalışanlarının sahip olduğu rollere, sorumluluklara, mesleki bilgi ve tecrübelere

göre onlara farklı düzeylerde erişim hakkı vermek için rol tabanlı erişim denetimi modelini kullanır [69, 70]. Bu teknik, hassas verileri korur ve çalışanların yalnızca ihtiyaç duydukları bilgilere erişmelerini ve işlerini yapmak için gerekli olan eylemleri gerçekleştirmelerini sağlar.

Bu erişim denetimi modelinde, her çalışana bir rol atanır ve bu rol sistemin kullanıcıya hangi izinleri vereceğini belirler. Örneğin, bir kullanıcının genel müdür mü, yönetici mi, uzman mı yoksa son kullanıcı mı olduğu belirlenir ve bu kullanıcıların bazı kaynaklara veya görevlere erişimi sınırlandırılır. Bir kuruluş, bazı kişilerin dosyaları oluşturmasına veya değiştirmesine izin verirken, diğerlerine yalnızca görüntüleme izni verebilir. Bazı durumlarda, kuruluşlar farklı rollere farklı düzeylerde izin verir veya izin düzeyleri çakışabilir [70].



Şekil 3.3 Rol tabanlı erişim denetimi modelinin yapısı

Şekil 3.3'te görüleceği üzere, bir rolün sahip olması gereken erişim parametreleri ve hangi kullanıcılara hangi rollerin atandığı bir yönetici tarafından belirlenir. Rol tabanlı erişim denetimi, kuruluşların güvenlik konusundaki duruşlarını iyileştirmelerine ve güvenlik denetimlerine uymalarına yardımcı olur. Modelin dezavantajı, bir kuruluşta rol tabanlı erişim denetimini uygulamak karmaşık bir hale gelebilir, çünkü ortakların arka planda kalmasına neden olabilir. Modele geçişte başarılı olmak için, aşağıda belirtilen uygulama süreçlerinin bir dizi adım olarak ele alınması gerekir [69, 70]:

- ***İş ihtiyaçlarını anlamak:*** Rol tabanlı erişim denetimi modeline geçmeden önce, iş süreçlerini ve teknolojileri destekleyen iş işlevlerini incelemek için kapsamlı bir ihtiyaç analizi yapılmalıdır. Ayrıca herhangi bir düzenleme veya denetim gerekliliğini göz önünde bulundurmalı ve kuruluşun mevcut güvenlik durumu değerlendirilmelidir. Diğer erişim kontrolü türlerinden de yararlanılmalıdır.
- ***Uygulama kapsamını planlama:*** Rol tabanlı erişim denetimi gereksinimlerinin kapsamının belirlenmesi ve uygulamanın kuruluşun ihtiyaçlarına göre planlanması gerekir. Hassas verileri depolayan sistemlere veya uygulamalara odaklanmak için kapsamın daraltılması da önemli bir husustur. Bu durum, kuruluşun geçişi yönetmesine de yardımcı olacaktır.
- ***Rolleri tanımlama:*** Gereksinimler belirlendikten ve kişilerin görev ve sorumluluklarını nasıl yerine getirecekleri tespit edildikten sonra rollerin tanımlanması gerekir. Aşırı veya yetersiz ayrıntı düzeyi, rol çakışması ve denetim modeli izinleri için çok fazla istisna verme gibi yaygın rol tasarımı tuzaklarına dikkat edilmesi gerekir.
- ***Uygulama:*** Son aşama, modelin kullanıma sunulmasını içerir. Aşırı bir iş yükünden kaçınmak ve işin aksamasını azaltmak için uygulamanın aşamalı olarak yapılması önemlidir. İlk olarak, çekirdek bir kullanıcı grubuna hitap edilmelidir. Ayrıca kullanıcılardan geri bildirim toplanması ve uygulamanın sonraki aşamalarını planlamak için ortamın izlenmesi gerekir.

Rol tabanlı erişim denetimi, siber güvenlik için de önemlidir, çünkü veri ihlallerine ilişkin istatistiklerde, personele uygun olmayan erişim seviyeleri verilmesinin veri kaybı ve veri hırsızlığının önde gelen bir nedeni olarak gösterilmektedir [9, 10, 21, 69, 70].

3.3.4 Öznitelik Tabanlı Erişim Denetimi

Öznitelik tabanlı erişim denetimi, "öznitelikler" adında bir dizi özelliğe dayanır. Bu özellikler, kullanıcı özniteliklerini, çevresel özniteliklerini ve kaynak özniteliklerini kapsar [71].

- ***Kullanıcı özniteliği***, kullanıcının adı, rolü, kuruluşu, kimliği ve güvenlik izni gibi şeyleri içerir.

- ***Çevresel öznitelik*** arasında erişim zamanı, verilerin konumu ve mevcut kurumsal tehdit seviyeleri bulunur.
- ***Kaynak özniteliği***, oluşturma tarihi, kaynak sahibi, dosya adı ve veri hassasiyeti gibi şeyleri içerir.

Öznitelikler, yetkilendirme amacıyla dikkate alınması gereken tüm varlıkları açıklamak için kullanılabilen etiket veya özellik kümeleridir. Her özellik, "Rol = Yönetici" gibi bir anahtar / değer çiftinden oluşur. Öznitelikler, statik değerlerle veya birbirleriyle karşılaştırılabilir (Şekil 3.4), böylece ilişki tabanlı erişim kontrolü sağlanır [71]. Merkezi bir politika, herhangi bir eylemi gerçekleştirmek için hangi kullanıcı ve nesne özellikleri kombinasyonlarının gerekli olduğunu tanımlar.

Şekil 3.4 Öznitelik tabanlı erişim denetimi modelinin yapısı

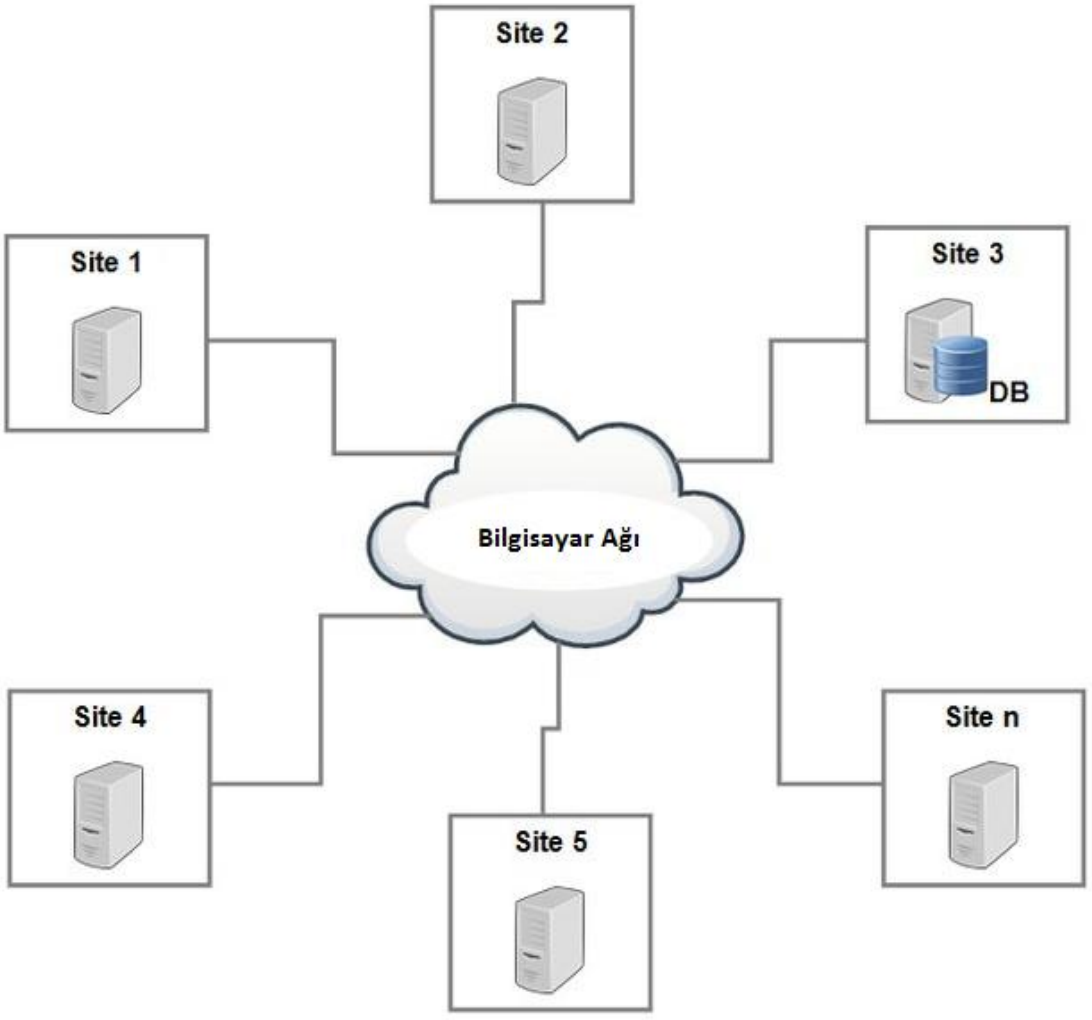
Bu yaklaşım, her büyüklükteki bir şirket için uygundur, ancak çoğunlukla büyük kuruluşlar için kullanılır [21, 66, 71]. Güvenlik yöneticilerinin sistemin tüm özniteliklerini tanımlaması gerektiğinden öznitelik tabanlı erişim kontrolü, dağıtım ve yapılandırma aşamasında rol tabanlı erişim kontrolü modelinden daha fazla zaman ve çaba gerektirir. İlk olarak, her bir sistem bileşenine manuel olarak öznitelikler atanması gerekir.

Esasen, öznitelik tabanlı erişim kontrolü, rol tabanlı erişim kontrolü modelinden çok daha fazla sayıda olası kontrol değişkenine sahiptir. Bu model, güvenliği ve erişimi daha ayrıntılı bir şekilde kontrol edebildiğinden, yetkisiz erişimden kaynaklanan riskleri azaltmak için uygulanır [72]. Örneğin, İK (İnsan Kaynakları) rolündeki kişilerin her zaman çalışan ve bordro bilgilerine erişebilmesi yerine, bu

erişim denetimi erişimlerine yalnızca belirli zamanlarda veya söz konusu çalışanla ilgili belirli şubeler için izin vermek gibi daha fazla sınırlama getirebilir. Bu, güvenlik sorunlarını azaltabilir ve ayrıca denetleme işlemlerine yardımcı olabilir.

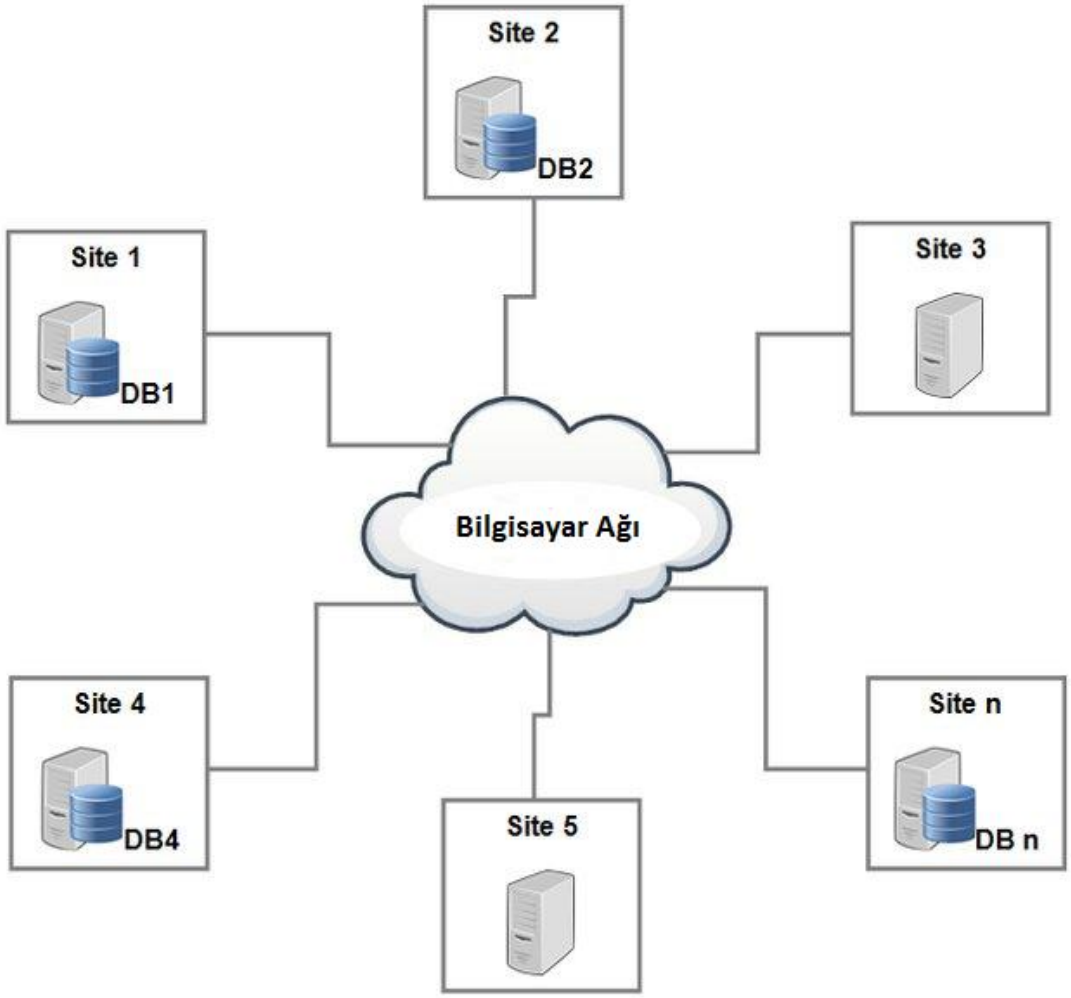
4
DAĞITIK VERİTABANI SİSTEMİ

Tüm verilerin depolandığı ve alındığı tek bir veri sunucusundan oluşan veritabanı merkezi olarak ifade edilir. Merkezi bir veritabanında tüm veriler tek bir konumda tutulur ve uygulamalar tüm verileri bu konumdan alır. Şekil 4.1'de merkezi veritabanı sisteminin bir mimari yapısı gösterilmiştir. Önceden tanımlanmış bir zaman diliminde, merkezi sunucudaki yönetim sistemi yazılımı, ülke geneline dağılmış yerel veri sunucularının her birinden veri ister [73].



Şekil 4.1 Merkezi veritabanı sisteminin mimarisi

Dağıtık bir veritabanı ise, aynı ağda bulunan farklı sitelerde veya tamamen farklı ağlarda bulunan iki veya daha fazla dosyadan oluşan bir veritabanıdır. Şekil 4.2'de dağıtık bir veritabanı ortamı gösterilmiştir. Veritabanının bölümleri birden çok fiziksel konumda saklanır ve işleme birden çok veritabanı düğümü arasında dağıtılır [73].



Şekil 4.2 Dağıtık veritabanı ortamı

Bir dağıtık veritabanı yönetim sistemi (Distributed Database Management System - DDBMS), verileri mantıksal olarak bütünleştirir, böylece tüm verileri aynı yerde depolanmış gibi yönetebilir.

DDBMS, tüm verileri periyodik olarak senkronize eder ve bir konumda gerçekleştirilen veri güncellemelerinin ve silme işlemlerinin, başka bir yerde depolanan verilere otomatik olarak yansıtılmasını sağlar [74].

4.1 Dağıtık Veritabanı Özellikleri

Bir koleksiyon içindeyken, dağıtık veritabanları mantıksal olarak birbirleriyle ilişkilidir ve genellikle tek bir mantıksal veritabanını temsil ederler. Dağıtık veritabanları ile veriler fiziksel olarak birden çok sitede depolanır ve bağımsız olarak yönetilir. Her sitedeki işlemciler bir ağ ile bağlanır ve herhangi bir çoklu işlem yapılandırması yoktur [75].

Genel olarak, dağıtık veritabanları aşağıdaki özellikleri içerir [75, 76]:

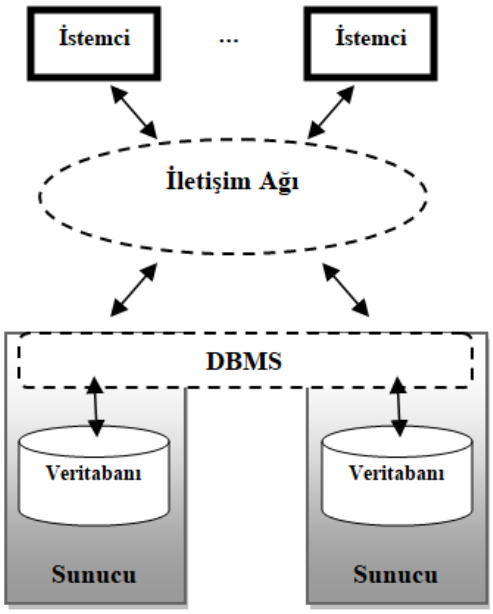
- Koleksiyondaki veritabanları mantıksal olarak birbirleriyle ilişkilidir. Genellikle tek bir mantıksal veritabanını temsil ederler.
- Veriler fiziksel olarak birden çok sitede depolanır. Her sitedeki veriler, diğer sitelerden bağımsız bir DDBMS tarafından yönetilebilir.
- Sitelerdeki işlemciler bir ağ üzerinden bağlanır. Çok işlemcili yapılandırmaları yoktur.
- Dağıtık veritabanı, gevşek bağlanmış bir dosya sistemi değildir.
- Dağıtık bir veritabanı işlem sürecini içerir, ancak bir işlem işleme sistemi ile eşanlamlı değildir.

4.2 Dağıtık Veritabanı Türleri

Genel olarak, dağıtık veritabanı sistemlerinin iki kategorisi vardır [76]: homojen veritabanı sistemi ve heterojen veritabanı sistemi.

4.2.1 Homojen Veritabanı Sistemi

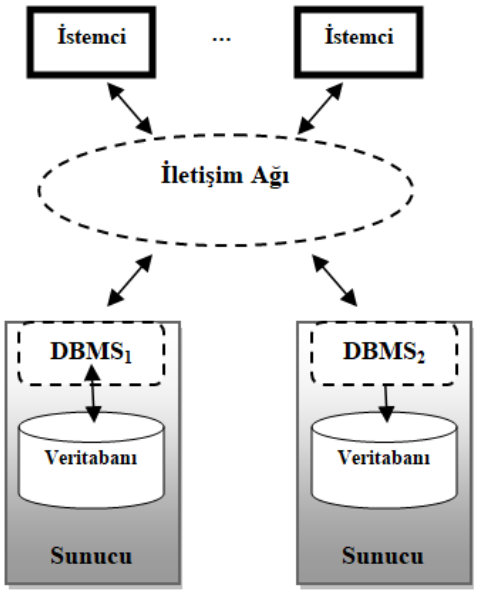
Tüm sunucular aynı veya uyumlu veritabanı yönetim sistemini kullanır ve kullanıcıya tek bir sistem olarak görünür. Bir veritabanının homojen yapıda olması için her konumdaki veri yapısının aynı veya uyumlu olması gerekir. Şekil 4.3'te homojen bir dağıtık veritabanı sistem yapısı gösterilmiştir. Bu yaklaşım ile, yeni bir sitenin dağıtık veritabanı yönetim sistemine kolayca eklenmesi ve birden fazla sitenin paralel işleme kapasitesinden faydalanarak performansını artırması sağlanır [76]. Avantajı, kullanımı, tasarımı ve yönetimi çok daha kolaydır. Dezavantajı, çoğu kuruluşların homojen ortamı zorlaması güçtür.



Şekil 4.3 Homojen dağıtık veritabanı sistemi

4.2.2 Heterojen Veritabanı Sistemi

Heterojen dağıtık bir veritabanında, donanım, işletim sistemleri veya veritabanı uygulamaları her konumda farklı olabilir. Şekil 4.4'te heterojen bir dağıtık veritabanı sistem yapısı gösterilmiştir. Her site, farklı şemalar ve yazılımlar kullanabilir. Siteler, birbirinin farkında olmayabilir ve işlemlerinde işbirliği için yalnızca sınırlı olanaklar sağlayabilir [76].



Şekil 4.4 Heterojen dağıtık veritabanı sistemi

Sistem, ana bilgisayarlar ve mikro bilgisayarlar gibi farklı bilgisayar sistemlerinde çalışan farklı veri modellerini (ilişkisel, hiyerarşik veya ağ) destekleyebilen farklı veritabanı yönetimi sistemlerini içerir. Avantajı, bir global merkezde farklı veri merkezinden gelen büyük veri depolanabilir, uzaktan erişim genel şema kullanılarak yapılır ve her düğümde farklı veritabanı yönetimi sistemleri kullanılabilir. Dezavantajı, yönetimi ve tasarımı zordur [77].

4.3 Avantajlar ve Dezavantajlar

Dağıtık Veritabanı Sistemlerinin bazı avantajlarını şöyle sıralayabiliriz [78, 79]:

- Sağlamlık: bir lokasyonda yaşanan sorunlar diğer lokasyonları aynı oranda etkilemez.
- Şirketin şubelerini birbirine bağlayan ağın geçici olarak kesintiye uğraması, yerel veritabanının çalışmasını kesintiye uğratmaz.
- Veri güvenliği: yalnızca yetkilendirilmiş personelin ihtiyacı olan verilere erişmesi sağlanır. Bu erişim, birtakım kısıtlamaları da içerebilir.
- Azaltılmış trafik ile ağın aşırı yüklenmemesi bant genişliği maliyetini düşürür.
- İyi ve yüksek performans: sorgular ve güncellemeler yerel olarak işlenir, böylece ağda daha fazla tıkanıklık olmaz.
- Bir lokasyonda gözlemlenen hatalar o lokasyonda tutulur ve tüm lokasyonları etkilemez.

Dağıtık Veritabanı Sistemlerinin bazı dezavantajlarını da şöyle sıralayabiliriz [78, 79]:

- Karmaşık uygulama: dağıtık bir veritabanı, kurulumunda ve bakımında belirli bir karmaşıklık sunar.
- Veri güvenliği: veri erişim noktalarının veya uzak sitelerin fazla olması, bu noktaların veya sitelerin güvenliğini garanti etmez.
- Veri bütünlüğü: verilere erişim yapan kullanıcı sayısı arttıkça, verilerin bozulma olasılığı da artar.
- Dağıtık veritabanı sistemlerinde veri verimliliğine ulaşabilmek için, verilerin dikkatlice yerleştirilmesi gerekir.

- Yine, dağıtık veritabanı sistemini verimli hale getirmek için siteler arasındaki etkileşimi önemli ölçüde azaltmalıyız.

4.4 Dağıtık Veri Depolama

Verilerin farklı sitelerde saklanmasının 2 yolu vardır [79]: Çoğaltma ve Parçalama.

4.4.1 Çoğaltma

Bu yaklaşımda, ilişkinin tamamı iki veya daha fazla sitede yedekli olarak depolanır. Veritabanının tamamı tüm sitelerde yer alıyorsa, bu veritabanı tamamen yedeklenmiş bir veritabanıdır. Bu nedenle, çoğaltmada sistemler verilerin kopyalarını tutar. Bu, farklı sitelerdeki verilerin kullanılabilirliğini artırdığı için avantajlıdır. Ayrıca sorgu istekleri paralel olarak işlenebilir [79, 80].

Ancak bazı dezavantajları da vardır. Verilerin sürekli güncellenmesi gerekir. Bir sitede yapılan herhangi bir değişikliğin, ilişkinin depolandığı her sitede kaydedilmesi gerekir, aksi takdirde tutarsızlıklara yol açabilir. Ayrıca, eşzamanlı erişim artık bir dizi site üzerinde kontrol edilmesi gerektiğinden, eşzamanlılık kontrolü daha karmaşık hale gelir [80].

4.4.2 Parçalama

Bu yaklaşımda, ilişkiler parçalanır (daha küçük parçalara ayrılırlar) ve parçaların her biri, gerekli oldukları yerde, farklı sitelerde depolanır. Parçaların, orijinal ilişkiyi yeniden yapılandırmak için kullanılabilecek şekilde olduğundan emin olunmalıdır (herhangi bir veri kaybı olmaz). Parçalanma, verilerin kopyalarını oluşturmadığı için avantajlıdır, tutarlılık bir sorun değildir [75, 79].

İlişkilerin parçalanması iki şekilde yapılabilir [75]:

- ***Yatay parçalama (Satırlara göre bölme):*** İlişki, her bir tuple en az bir parçaya atanacak şekilde tuple gruplarına ayrılır.
- ***Dikey parçalama (Sütunlara göre bölme):*** İlişkinin şeması daha küçük şemalara bölünmüştür. Kayıpsız birleştirmeyi sağlamak için her parça ortak bir aday anahtar içermelidir.

4.5 Dağıtık Veritabanlarında Güvenlik

Dağıtık bir sistem, merkezi sisteme göre ek güvenlik önlemlerine ihtiyaç duyar, çünkü çok sayıda kullanıcı, çeşitlendirilmiş veri, birden fazla site ve dağıtık kontrol vardır. Dağıtık iletişim sistemlerinde, iki tür davetsiz misafir vardır [75, 79]: pasif dinleyiciler ve aktif saldırganlar.

- Pasif dinleyiciler: Mesajları izler ve özel bilgileri ele geçirirler.
- Aktif saldırganlar: Yalnızca iletileri izlemekle kalmaz, aynı zamanda yeni veriler ekleyerek veya mevcut verileri değiştirerek verileri bozarlar.

Güvenlik önlemleri, iletişimde güvenliği, veri güvenliğini ve veri denetimini kapsar [79].

4.5.1 İletişim Güvenliği

Dağıtık bir veritabanında, verilerin, kullanıcıların ve işlemlerin çeşitlendirilmiş konumu nedeniyle çok fazla veri iletişimi gerçekleşir. Bu nedenle, kullanıcılar, veritabanları ve farklı veritabanı ortamları arasında güvenli iletişim gerekir [81].
İletişim güvenliği şunları kapsar [79, 81]:

- Aktarım sırasında veriler bozulmamalıdır. Veri bütünlüğü korunmalıdır.
- İletişim kanalı hem pasif dinleyicilere hem de aktif saldırganlara karşı korunmalıdır.
- Yukarıda belirtilen gereksinimleri karşılamak için, iyi tanımlanmış güvenlik algoritmaları ve protokolleri benimsenmelidir.

Ayrıca, uçtan uca güvenli iletişim sağlamak için iki popular ve tutarlı teknoloji vardır [74, 79, 80]: Güvenli Soket Katmanı Protokolü veya Taşıma Katmanı Güvenliği Protokolü ve Sanal Özel Ağlar (VPN).

4.5.2 Veri Güvenliği

Dağıtık sistemlerde, verileri iletişim dışında güvence altına almak için önlem almak zorunludur. Veri güvenliği önlemleri şunlardan oluşur [74, 80, 81]: kimlik doğrulama ve yetkilendirme, veri şifreleme ve doğrulanmış giriş.

- ***Kimlik doğrulama ve yetkilendirme:*** Bunlar, yalnızca gerçek kullanıcıların veri tabanını kullanabilmesini sağlamak için benimsenen erişim kontrol

tedbirleridir. Kimlik doğrulamayı sağlamak için dijital sertifikalar kullanılır. Ayrıca kullanıcı adı / şifre kombinasyonu ile giriş kısıtlanmaktadır.

- ***Veri şifreleme:*** Dağıtık sistemlerde veri şifreleme için iki yaklaşım vardır:

  1) *Dahili dağıtık veritabanı yaklaşımı:* Kullanıcı uygulamaları, verileri şifreler ve ardından şifrelenmiş verileri veri tabanında depolar. Depolanan verileri kullanmak için, uygulamalar şifrelenmiş verileri veritabanından alır ve ardından şifresini çözer.

  2) *Harici dağıtık veritabanı yaklaşımı:* Dağıtık veritabanı sisteminin kendi şifreleme yetenekleri vardır. Kullanıcı uygulamaları, verileri depolar ve verilerin veritabanında şifrelenmiş bir biçimde depolandığının farkına varmadan geri alır.

- ***Doğrulanmış giriş:*** Bu güvenlik önleminde, kullanıcı uygulaması, veri tabanını güncellemek için kullanılmadan önce her girişi kontrol eder. Doğrulanmamış bir girdi, arabellek taşması, komut enjeksiyonu, siteler arası komut dosyası oluşturma ve verilerde bozulma gibi çok çeşitli istismarlara neden olabilir.

4.5.3 Veri Denetimi

Bir veritabanı güvenlik sistemi, alması gereken güvenlik önlemlerini tespit etmek için öncelikli olarak güvenlik ihlallerini tespit etmeli ve izlemelidir. Güvenlik ihlallerini olaylar anında tespit etmek genellikle çok zordur. Güvenlik ihlallerini belirlemenin bir yolu, denetim günlüklerini incelemektir. Denetim günlükleri şu bilgileri içerir [74, 81]:

- Başarısız erişim girişimlerinin tarihi, saati ve sitesi.
- Başarılı erişim girişimlerinin ayrıntıları.
- Veritabanı sistemindeki hayati değişiklikler.
- Özellikle birden çok sitedeki veritabanlarından büyük miktarda veriye erişim.

Yukarıdaki bilgilerin tümü, veri tabanındaki faaliyetler hakkında bir fikir verir. Günlüğün periyodik analizi, herhangi bir doğal olmayan etkinliği, sitesi ve oluşma

zamanıyla birlikte tanımlamaya yardımcı olur. Bu günlük ideal olarak ayrı bir sunucuda depolanır, böylece saldırganlar tarafından erişilemez [74, 81].

5
ÖNERİLEN ERİŞİM DENETİMİ MODELİ

Yargı ağı sistemleri, savunma sistemleri ve hastane yönetim sistemleri gibi statik erişim denetimi modellerinin etkili olmadığı birçok gerçek dünya uygulaması vardır. Örneğin, gizliliğin, güvenlik kısıtlamalarının ve erişim düzeyinin organizasyon yapısına göre farklılık göstermesi, başlangıçta karar verilen güvenlik politikalarının değişen kurumsal ya da ticari koşullara ve iş gereksinimlerine uygun bir şekilde dinamik olarak değiştirilememesi ve erişim denetimlerinin kolay yönetilememesi gibi [4, 6, 14, 16, 20].

Bu tez çalışması kapsamında, gerçek sistem uygulamalarında deneyimlediğimiz bu tür sorunlar referans alınarak; farklı sistemlere uyarlanabilen, kullanıcı ve nesnenin organizasyon yapısı içerisindeki mevcut durumunu ve zaman içerisinde değişen veya güncellenen durumlarını (izin seviyesi, birtakım ayrıcalıklar, istisnai durumlar, gizlilik derecesi, vb.) baz alarak kullanıcının nesne üzerindeki izin ve erişim düzeyinin dinamik olarak değiştirilmesini sağlayan dinamik bir erişim denetimi modeli sunulmuştur.

5.1 Güvenlik Boyutu

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 5.1'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.

Tablo 5.1 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.

Bir organizasyon içerisinde en yetkili ve/veya eşdeğer yetkilere sahip olan kişi ya da gruplar tarafından kullanıcılara boyut değerleri atanır. Her kullanıcıya her boyuttan en az bir değer atanmış olmalıdır. Ancak bazı boyutlardan birkaç değer atanabilir. Örneğin, Tablo 5.2'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.

Tablo 5.2 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*

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/veya 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.

5.2 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.

5.3 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 ***Yalnızca Yazma*** ise, Nesne görüntülenemez, ancak değiştirilebilinir.

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

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

5.4 Özel Erişim İzni Oluşturma

Önerilen erişim denetimi modeli ile, istisnai onay mekanizmasını işleterek sektör uygulamalarına esneklik kazandırmak, böylece mevcut uygulamaların kaynak kullanılabilirliğini ve iş zamanı verimliliğini artırabilmek amaçlanmıştır. Bunun için de gerektiğinde ve bazı özel durumlarda kullanıcılara geçici ya da kalıcı birtakım özel erişim izinleri (özel hak ve yetkiler) getirilmiştir.

Bir nesne, bir kullanıcıyı en az bir izin düzeyiyle ilişkilendirmek için herhangi bir izne sahip olmadığında, erişim izni "Yok" izin düzeyiyle sonuçlanır. Bu durumda kullanıcı o nesneyi görüntüleyemez ve değiştiremez. Fakat bir kullanıcının, bir nesne için erişim izni alması gerektiği özel durumlarda, nesnenin sahip olduğu izin listesine kullanıcının sahip olduğu en az bir güvenlik boyutu özelliğinin eklenmesi ve kullanıcının en az bir güvenlik boyutu özelliğinin "İzin verildi" izin düzeyiyle ilişkilendirilmesi gerekmektedir. Bir örnek üzerinden bu durumu anlatacak olursak;

Tablo 5.3'te bir kullanıcıya atanmış boyut değerleri gösterilmiştir.

Tablo 5.3 Kullanıcı3'e tanımlanmış boyut değerleri

Güvenlik Boyutu	Kullanıcı3
Birim	*Birim D*
Güvenlik Sınıflandırması	*Özel*
İş Unvanı	*Hemşire*
Operasyon	*İşlem C, D, E*

Nesne, Tablo 5.4'te gösterilen şu izin ya da izinlere sahip olabilir:

Tablo 5.4 Bir nesneye ait örnek erişim izinleri - 1

Güvenlik Boyutu	Boyut Değeri	İzin Düzeyi
Güvenlik Sınıflandırması	*Gizli*	İzin verildi
İş Unvanı	*BT Personeli*	İzin verildi

Tablo 5.3'te kullanıcının Güvenlik Sınıflandırması özelliğinin "Özel" güvenlik boyutu değerinde yer aldığı görülmektedir. Nesne, Güvenlik Sınıflandırması yalnızca "Gizli" güvenlik boyutu değerinde olan bir izin düzeyiyle ilişkilendirildiğinden ve Güvenlik Sınıflandırması "Özel" olan bir izin düzeyine sahip olmadığından, bu kullanıcının erişim izni "Yok" izin düzeyiyle sonuçlanır.

Kullanıcının, ilgili nesne için erişim iznine sahip olabilmesinin yolu, nesnenin erişim izinleri listesine kullanıcının en az bir güvenlik boyutu özelliğinin eklenip, en az bir güvenlik boyutu özelliğinin bir izin düzeyiyle ilişkilendirilmesine bağlıdır. Örneğin Tablo 5.5'e kullanıcının Operasyon güvenlik boyutundaki "İşlem C" özelliği nesnenin erişim izinleri listesine eklenip, izin düzeyi de "İzin verildi" ile ilişkilendirildiğinde, bu defa kullanıcının erişim izni "İzin verildi" izin düzeyiyle sonuçlanır. Bu durum, özel erişim izni oluşturmanın bir sonucudur.

Tablo 5.5 Bir nesneye ait örnek erişim izinleri - 2

Güvenlik Boyutu	Boyut Değeri	İzin Düzeyi
Güvenlik Sınıflandırması	*Gizli*	İzin verildi
İş Unvanı	*BT Personeli*	İzin verildi
Operasyon	***İşlem C***	**İzin Verildi**

5.5 Erişim ve İzin Düzeylerini Hesaplama

Bir nesneye erişim izni, boyut değerleri (kullanıcının her bir boyutta almış olduğu değerdir, örneğin Tablo 5.2'de 5 farklı kullanıcıya tanımlanmış değerler gibi) ve erişim düzeyi (Okuma/Yazma, Yalnızca Okuma, Yalnızca Yazma, 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.

5.5.1 Bir Boyuttaki Erişim Düzeyini ve 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; Tablo 5.6'da bir kullanıcıya atanmış boyut değerleri gösterilmiştir.

Tablo 5.6 Kullanıcı1'e tanımlanmış boyut değerleri

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

Bu kullanıcı, Tablo 5.7'de gösterilen şu erişim izinlerine sahip nesneyi görüntülemek isteyebilir:

Tablo 5.7 Bir nesneye ait erişim düzeyleri

Güvenlik Boyutu	Boyut Değeri	Erişim Düzeyi
Birim	*Birim E*	Yalnızca Okuma

Tablo 5.7 Bir nesneye ait erişim düzeyleri (devamı)

Güvenlik Sınıflandırması	*Gizli*	Yalnızca Yazma
Güvenlik Sınıflandırması	*Özel*	Yalnızca Okuma
Güvenlik Sınıflandırması	*Özel*	Örtülü
Operasyon	*İşlem A*	Okuma
Operasyon	*İşlem D*	Okuma / Yazma

Nesne, Tablo 5.8'de gösterilen şu izin ya da izinlere sahip olabilir:

Tablo 5.8 Nesnenin erişim izni / izinleri

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 C için tanımlanmış bir erişim izni olmadığından, Operasyon boyutundaki İşlem C 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" olan Güvenlik Sınıflandırması boyut değerlerinden en az kısıtlayıcı olan *Yalnızca Okuma* erişimiyle sonuçlandığını belirtir.

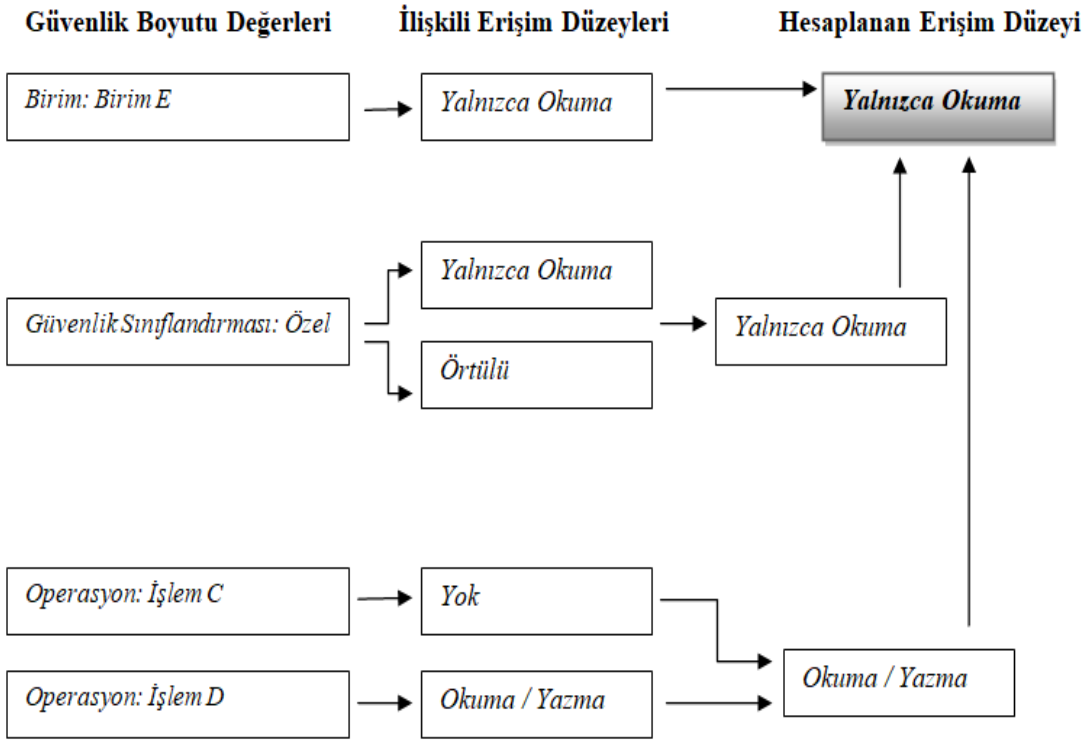
Nesne, "Hemşire" İş Unvanı güvenlik boyutunu bir izin düzeyiyle ilişkilendirmek için herhangi bir izne sahip olmadığından, sonuç "Yok" izin düzeyidir.

5.5.2 Nesne Üzerindeki Genel Erişim ve İzin Düzeyini Hesaplama

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

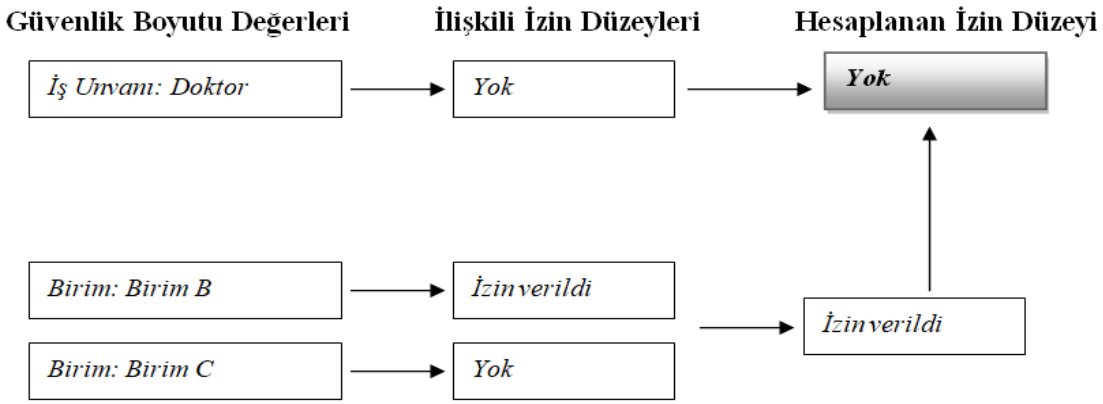
Şekil 5.1'de genel erişim düzeyinin hesaplanması gösterilmiştir. Birim boyutu için Yalnızca Okuma erişim düzeyi, Operasyon boyutu için Okuma ve Yazma erişim düzeyi, Güvenlik Sınıflandırması boyutu için ise Yalnızca Okuma erişim düzeyi

kullanılır. Bu farklı düzeylerin en kısıtlayıcısı Yalnızca Okuma olduğundan, kullanıcının nesnede aldığı genel erişim düzeyi ***Yalnızca Okuma*** olur.



Şekil 5.1 Genel erişim düzeyi hesaplama

Benzer hesaplama yöntemi izin düzeyleri için de geçerlidir. Her boyuttan en az kısıtlayıcı izin düzeyi alınırken, farklı boyutlardan gelen düzeylerden ise en kısıtlayıcı olan izin düzeyi alınır ve böylece genel izin düzeyi belirlenmiş olunur. Yukarıdaki örnekten bağımsız olarak Şekil 5.2'de genel bir izin düzeyi hesaplama yöntemi gösterilmiştir.

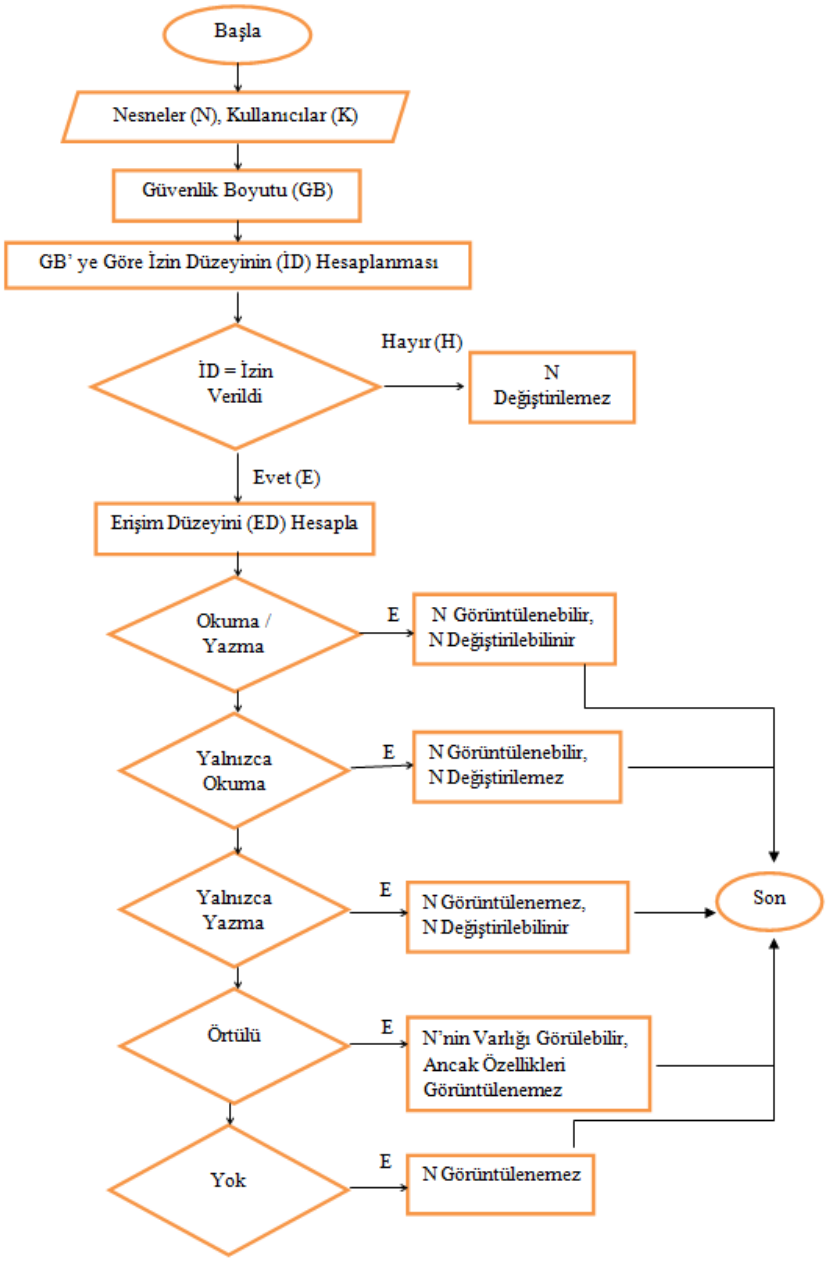


Şekil 5.2 Genel izin düzeyi hesaplama

Ayrıca, bir kullanıcı için tanımlanmış güvenlik boyutları ve nesnenin izin ve erişim düzeylerinde herhangi bir değişiklik yok ise kullanıcının aynı nesne üzerindeki genel erişim izni ve düzeyi bir kez hesaplanır, aynı nesne için ikinci ve daha fazla kez erişim izni ve düzeyi hesaplanmaz, kullanıcının aynı nesne için erişim talebi daha önce hesaplanan izin ve erişim düzeyi ile birlikte değerlendirilir.

5.6 Önerilen Modelin Akış Şeması

Önerdiğimiz modelin akış şeması Şekil 5.3'te gösterilmektedir.



Şekil 5.3 Önerilen modelin akış şeması

6
DENEYSEL SONUÇLAR

Bu tez çalışmasında, sağlık, eğitim ve kamu sektörlerinde yer alan kurum ve kuruluşlardan alınmış üç farklı gerçek veri seti kullanılmıştır. Önerilen erişim denetimi modeli ve diğer erişim denetimi modellerinin (Rol Tabanlı Erişim Denetimi, Öznitelik Tabanlı Erişim Denetimi ve Zorunlu ve İsteği Bağlı Erişim Denetimi) başarısı her bir veri setinden elde edilen performans sonuçlarına göre değerlendirilmiştir.

6.1 Veri Kümeleri

Çalışmada kullanılan farklı sektörlerden alınmış üç veri seti ön işlemden geçirilmiş ve her bir kullanıcı güvenlik boyutlarına göre sınıflandırılmıştır. Kullanıcıların güvenlik boyutlarına göre sınıflandırılması işleminde, verisetlerinin alındığı kurum ve kuruluşların iç ve dış denetim raporlarında geçen erişim izni ve düzeyi kuralları baz alınmıştır. İç ve dış denetim raporları doğrultusunda oluşturulmuş kurallar çerçevesinde özel olarak geliştirilmiş bir algoritma ile kullanıcılara farklı güvenlik boyutlarından değer atamaları yapılmıştır. Nesnelerin izin ve erişim düzeyleri ise, kullanıcıların nesne üzerinde hesaplanan genel izin ve erişim düzeylerine göre belirlenmiştir. Bu belirleme işleminde de kurum ve kuruluşların denetim raporları baz alınmış ve her nesnenin izin ve erişim düzeyleri aynı algoritma tarafından otomatik olarak hesaplanmıştır.

Sağlık sektöründen alınan veri kümesi 107 kullanıcı, 36.251 nesne ve 8 güvenlik boyutundan (Tablo 6.1), Eğitim sektöründen alınan veri kümesi 292 kullanıcı, 72.988 nesne ve 6 güvenlik boyutundan (Tablo 6.2) ve Kamu sektöründen alınan veri kümesi 1.355 kullanıcı, 752.220 nesne ve 11 güvenlik boyutundan (Tablo 6.3) oluşmaktadır. Çalışmada veri setleri “Sağlık Veri Seti”, “Eğitim Veri Seti” ve “Kamu Veri Seti” olarak ifade edilmiştir.

Tablo 6.1 Sağlık veri seti güvenlik boyutu ve sayısı

Güvenlik Boyutu	Sayı
İl	81
Hastane	68
Birim	41
İş Unvanı	27
Eğitim Düzeyi	8
Kıdem	5
Referans	2
Güvenlik Sınıflandırması	5

Tablo 6.2 Eğitim veri seti güvenlik boyutu ve sayısı

Güvenlik Boyutu	Sayı
İl	81
İlçe	922
Okul	1205
İş Unvanı	13
Eğitim Düzeyi	8
Güvenlik Sınıflandırması	4

Tablo 6.3 Kamu veri seti güvenlik boyutu ve sayısı

Güvenlik Boyutu	Sayı
İl	81
Kurum	101
Birim	28
İş Unvanı	21
Eğitim Düzeyi	8
Kıdem	3
Referans	3
Operasyon	7
Kimlik Doğrulama Türü	5
Faaliyet	12
Güvenlik Sınıflandırması	5

6.2 Performans Ölçütü

Önerilen model ve diğer erişim denetimi modelleri gerçek bir dağıtık sistem sunan bir platform üzerinde çalıştırılmış ve tüm erişim denetimi modelleri üç veri setine ayrı ayrı uygulanmıştır. Her bir veri setine ayrı ayrı uygulanan erişim denetimi modelleri için elde edilen izin ve erişim düzeyi sonuçları, veri setinin alındığı kurum ve kuruluşlara ait uygulamalarda geçerli kılınan izin ve erişim düzeyi sonuçları ile karşılaştırılmıştır. Daha sonra önerilen model ile çalışmada ele aldığımız diğer modellerin performans değerleri karşılaştırmalı olarak analiz edilmiştir.

Performans değerlerinin nasıl hesaplandığı aşağıda verilen bir örnek üzerinden gösterilmiştir.

Tablo 6.4 Hesaplanan erişim izni ve düzeyi sonuçları

Veri Seti: Sağlık	**Nesne No : 1**	**Kullanıcılar**	**İzin Düzeyi**	**Erişim Düzeyi**
		Kullanıcı 1	İzin Verildi	Yalnızca Okuma
		Kullanıcı 2	İzin Verildi	Okume ve Yazma
		Kullanıcı 3	Yok	Yok
		Kullanıcı 4	İzin Verildi	Yalnızca Yazma

Tablo 6.5 Sektörde geçerli olan gerçek erişim izni ve düzeyi sonuçları

Veri Seti: Sağlık	**Nesne No : 1**	**Kullanıcılar**	**İzin Düzeyi**	**Erişim Düzeyi**
		Kullanıcı 1	İzin Verildi	Yalnızca Okuma
		Kullanıcı 2	İzin Verildi	Okume ve Yazma
		Kullanıcı 3	Yok	Yok
		Kullanıcı 4	İzin Verildi	***Okuma ve Yazma***

Tablo 6.4'te Sağlık veri setinde yer alan "1" numaralı nesne için hesaplanan erişim izni ve düzeyi sonuçları gösterilmiştir. Tablo 6.5'te ise Sağlık veri setinde "1" numaralı nesne için geçerli olan erişim izni ve düzeyi sonuçları gösterilmiştir. Her iki tablo karşılaştırıldığında; hesaplanan erişim izinleri, geçerli olan erişim izinleri ile %100 örtüşürken, hesaplanan erişim düzeyinde ise Kullanıcı 4 için tespit edilen erişim düzeyinin hatalı olduğu, yani Kullanıcı 4 için geçerli olan erişim düzeyi

"Okuma ve Yazma" iken, hatalı olarak erişim düzeyi "Yalnızca Yazma" olarak hesaplandığı tespit edilmektedir. Bu durumda, "1" numaralı nesne için hesaplanan erişim izninin doğruluk oranı %100 iken, hesaplanan erişim düzeyinin doğruluk oranı %75 olacaktır.

Her bir veri kümesine uygulanan erişimi denetimi modellerinin performans değerlendirilmesinde, her modelin doğru izin ve erişim düzeyi tespit etme başarısı esas alınmıştır.

6.3 Önerilen Modelin Performans Sonuçları

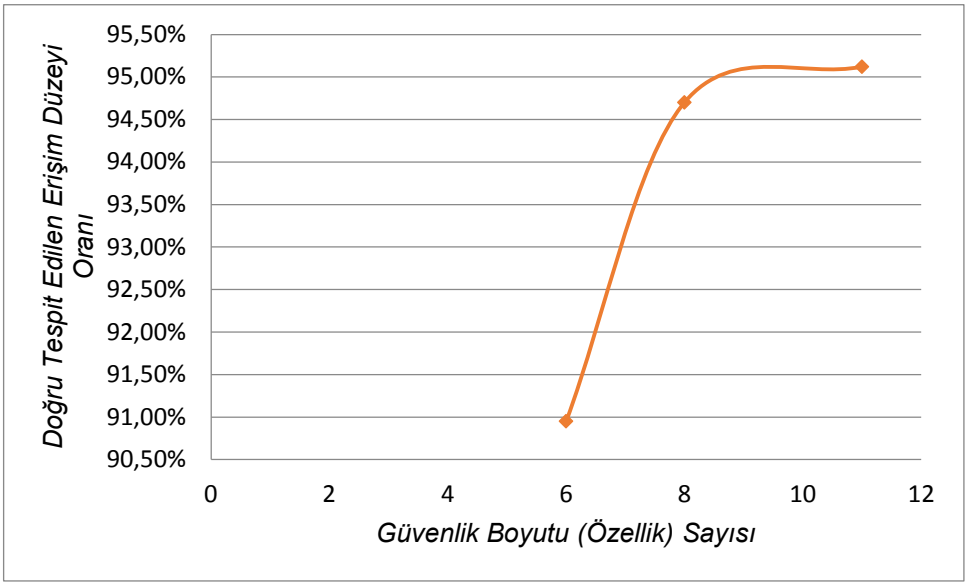
Önerilen modelin, sağlık, eğitim ve kamu veri setleri üzerindeki test sonuçları Tablo 6.6'da gösterilmiştir. Önerilen model ile, Sağlık veri seti için %98,20 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %94,70'inde erişim düzeyinin doğru tespit edildiği, Eğitim veri seti için %95,03 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %90,95'inde erişim düzeyinin 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 düzeyinin doğru tespit edildiği test edilmiştir.

Tablo 6.6 Önerilen modelin izin 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 sonuçlarını sunduğunu söyleyebiliriz. Ayrıca güvenlik boyutu (özellik sayısı) arttıkça erişim düzeyinde tespit edilen başarı oranının da arttığı, nitekim Şekil 6.1'de görüleceği üzere 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 kıyasla fazla olmasının etkili olduğu gözlenmiştir.



Şekil 6.1 Güvenlik boyutu sayısına göre erişim düzeyi başarı oranı

6.4 Rol Tabanlı Erişim Denetimi Modelinin Performans Sonuçları

Rol Tabanlı Erişim Denetimi modelinin, sağlık, eğitim ve kamu veri setleri üzerindeki test sonuçları Tablo 6.7'de 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 düzeyinin 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 düzeyinin 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 düzeyinin doğru tespit edildiği test edilmiştir.

Tablo 6.7 İzin ve erişim düzeyi performansı (RBAC)

	Erişim İzni	**Erişim Düzeyi**
Sağlık Veri Seti	92,17%	90,63%

Tablo 6.7 İzin ve erişim düzeyi performansı (RBAC) (devamı)

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 sonuçlarını sunduğu, özellikle kullanıcı ve nesne sayısı arttıkça erişim düzeyindeki doğruluk oranında azalma gözlendiği test edilmiştir.

6.5 Öznitelik Tabanlı Erişim Denetimi Modelinin Performans Sonuçları

Öznitelik Tabanlı Erişim Denetimi modelinin, sağlık, eğitim ve kamu veri setleri üzerindeki test sonuçları Tablo 6.8'de gösterilmiştir. Bu model ile, Sağlık veri seti için %93,15 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %92,94'ünde erişim düzeyinin doğru tespit edildiği, Eğitim veri seti için %89,90 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %87,35'inde erişim düzeyinin doğru tespit edildiği ve Kamu veri seti için %89,62 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %87,20'sinde erişim düzeyinin doğru tespit edildiği test edilmiştir.

Tablo 6.8 izin ve erişim düzeyi performansı (ABAC)

	Erişim İzni	**Erişim Düzeyi**
Sağlık Veri Seti	93,15%	92,94%
Eğitim Veri Seti	89,90%	87,35%
Kamu Veri Seti	89,62%	87,20%

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

6.6 Zorunlu ve İsteği Bağlı Erişim Denetimi Modellerinin Performans Sonuçları

Zorunlu ve İsteği Bağlı Erişim Denetimi modellerinin, sağlık, eğitim ve kamu veri setleri üzerindeki test sonuçları Tablo 6.9'da gösterilmiştir. Bu iki 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 modeller ile, Sağlık veri seti için %87,60 oranında izin düzeyinin doğru bulunduğu, izin düzeyi doğru tespit edilen nesnelerin ise %86,02'sinde erişim düzeyinin 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 düzeyinin 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 düzeyinin doğru tespit edildiği test edilmiştir.

Tablo 6.9 İzin ve erişim düzeyi performansı (MAC/DAC)

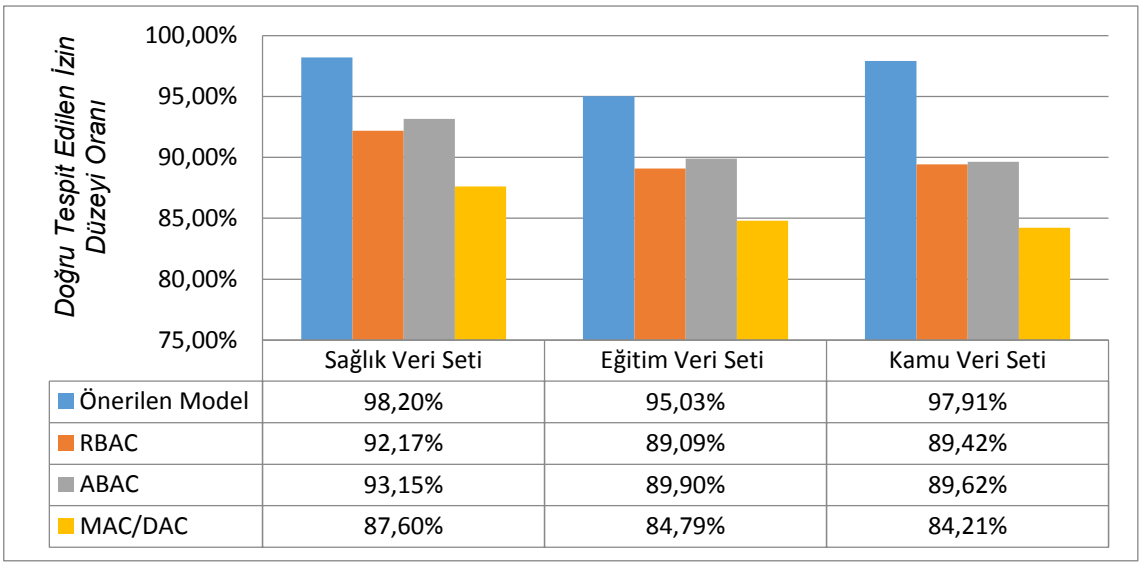
	Erişim İzni	**Erişim Düzeyi**
Sağlık Veri Seti	87,60%	86,02%
Eğitim Veri Seti	84,79%	81,39%
Kamu Veri Seti	84,21%	79,54%

MAC/DAC modellerinin sunduğu sonuçlar değerlendirildiğinde, tıpkı ABAC ve 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 sonuçlarını sunduğu, özellikle kullanıcı ve nesne sayısı arttıkça erişim ve izin düzeyindeki doğruluk oranında azalma gözlendiği test edilmiştir.

6.7 Grafiksel Performans Değerlendirme

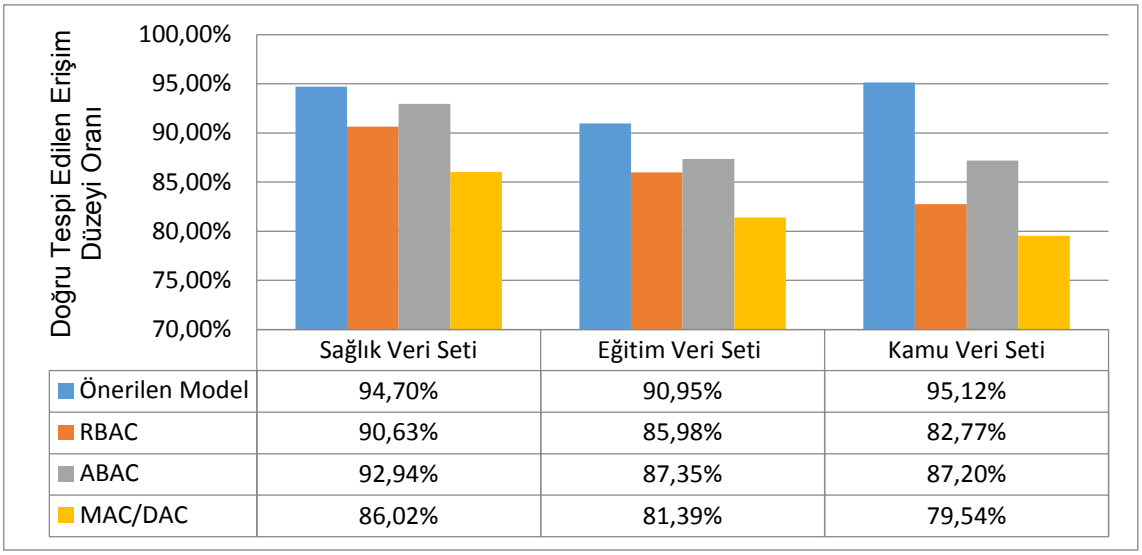
Önerdiğimiz modelin, diğer tekniklere oranla erişim izni ve erişim düzeyi tespitinde daha başarılı sonuçlar verdiği test edilmiştir. Şekil 6.2 ve Şekil 6.3'te görüleceği üzere önerilen modelimizin özellikle her üç veri setinde %90 ve

üzerinde doğru erişim izni ve düzeyi tespit etme oranını yakaladığı, diğer tekniklerin ise kullanıcı ve nesne sayısı yüksek veri setlerinde önerilen modelimize kıyasla daha düşük doğru tespit etme oranına ulaştığı gözlenmiştir.



	Sağlık Veri Seti	Eğitim Veri Seti	Kamu Veri Seti
Önerilen Model	98,20%	95,03%	97,91%
RBAC	92,17%	89,09%	89,42%
ABAC	93,15%	89,90%	89,62%
MAC/DAC	87,60%	84,79%	84,21%

Şekil 6.2 Modellerin erişim izni doğru tespit oranı



	Sağlık Veri Seti	Eğitim Veri Seti	Kamu Veri Seti
Önerilen Model	94,70%	90,95%	95,12%
RBAC	90,63%	85,98%	82,77%
ABAC	92,94%	87,35%	87,20%
MAC/DAC	86,02%	81,39%	79,54%

Şekil 6.3 Modellerin erişim düzeyi doğru tespit oranı

Grafiksel veriler bir bütün olarak değerlendirildiğinde, modelimizin diğer teknikler karşısında farklı sektör uygulamaları için daha genişletilebilir ve aynı sektör uygulamaları için de daha ölçeklenebilir bir teknik sunduğunu söyleyebiliriz.

6.8 Erişim Süresi Performansı

Çalışmada genel izin ve erişim düzeyleri hesaplanırken aynı zamanda modellerin veri erişim süreleri de hesaplanmıştır. Her bir model, her bir veri setine 10 kez uygulanmış olup, her bir model için alınan 10 farklı erişim süresinin aritmatik ortalaması hesaplanarak her bir modelin ortalama erişim süreleri belirlenmiştir. Her bir veri setinde her bir model için hesaplanan ortalama erişim sürelerine Tablo 6.10'da yer verilmiştir.

Tablo 6.10 Erişim süreleri (dakika)

	Sağlık Veri Seti	**Eğitim Veri Seti**	**Kamu Veri Seti**
Önerilen Model	1:20	1:48	2:52
RBAC	1:16	1:52	2:40
ABAC	1:35	2:01	2:54
MAC	0:57	1:27	1:55
DAC	1:09	1:29	2:07

Önerilen modelin, her üç veri setindeki ortalama erişim süresinin yaklaşık 1 ila 3 dakika arasında değiştiği, ABAC modeline göre kıyaslarsak daha iyi bir erişim süresi sunduğu, özellikle veri sayısı arttıkça erişim sürelerinin de yaklaşık benzer oranlarda arttığı gözlenmiştir.

Gelecek çalışmalarda, önerilen model geliştirilerek erişim denetiminde veri erişim sürelerini ve gecikmeyi azaltacak yeni bir çerçeve model sunulacaktır.

7
SONUÇ VE ÖNERİLER

Siber güvenlik alanının neredeyse tamamen kimlik doğrulama ve erişim denetimine dayandığına dair güçlü bir argüman vardır. Bu iki işlev olmadan, neredeyse hiçbir güvenlik tekniği önemli değildir. Diğer her güvenlik unsuru, kullanıcıyı tanımlayan ve çeşitli nesnelere yönelik izinleri doğrulayan bir sisteme bağlıdır.

BT güvenliği tartışmalarında, erişimi yönetmeyi ve kullanıcıları tanımlamayı amaçlayan projeler temel kabul edilir. Bununla birlikte, izinleri kontrol etmek için süreçler ve teknolojiler hep zorlayıcı olmuştur. Erişim kontrolü olmadığında, kaynakların yalnızca hedef kullanıcıları tarafından kullanıldığını garanti etmek neredeyse imkansızdır. İzin yönetiminin olmaması durumunda, kullanıcıların ihtiyaç duymadığı bilgi ve hizmetlere erişmesine izin verilir. Başka bir deyişle, uygunsuz veri erişimlerine ve olası uygulama arızalarına yol açılır. Bu durum, milyonlarca dolara mal olan veri ihlallerine ve itibarın zarar görmesine de neden olabilir.

Bilgi değerli bir varlıktır. Gizliliğin, bütünlüğün ve erişebilirliğin sürdürülebilir olduğundan emin olmak için bilgilere erişim dikkatle yönetilmelidir. Literatürde son yıllarda bilgi ve bilgi sistemlerine erişimi, yetkilendirme, izleme ve kontrol etme ile ilgili kuralları ana hatlarıyla belirleyen bazı teknikler geliştirilmiştir. Bu tekniklerin çoğunlukla bulut bilişim, büyük veri ve nesnelerin interneti gibi yenilikçi teknoloji alanlarını kapsadığı görülmektedir. Oysa birçok sektörde karşılaştığımız dağıtık veritabanı sistemini kullanan bilgi ve iletişim teknolojileri uygulamalarında erişim denetimi tekniklerinin gelişim süreçlerinin yavaşladığı, varolan tekniklerin gelişen teknoloji ile birlikte ortaya çıkan yeni iş gereksinimlerini tam olarak karşılamadığı ve organizasyon yapısına uygun bir şekilde yönetilemediği, yönetilebilir bir erişim denetimi modeline doğru

ilerlemelerde ciddi maliyetlerin ortaya çıktığı, kaynakların kullanımı ve paylaşımı konusunda gerekli olan dinamizme ulaşılamadığı görülmektedir.

Bu tez çalışmasında her kullanıcıya organizasyon yapısına uygun bir şekilde tanımlanmış farklı güvenlik boyutlarında birçok değer (özellik) atanır. Kullanıcının dağıtık ortamdaki bir nesneye erişim izni; istisnai erişim onayları, kullanıcının sahip olduğu boyut değerleri ve nesne erişim düzeyleri ile ilişkilendirilir. Yani bir kullanıcının sahip olduğu özel erişim iznine ve/veya yetkilere, kendisine atanmış boyut değerlerine ve nesnenin sahip olduğu erişim düzeylerine göre o kullanıcının bir nesne üzerindeki erişim izni ve düzeyi dinamik olarak hesaplanır.

Çalışmada ele aldığımız önerilen erişim denetimi modeli, gerçek bir dağıtık ortam sunan bir platformlar üzerinde çalıştırılmış, böylece farklı fiziksel ortamlarda saklanan verilere kullanıcıların hangi erişim izni ve düzeyi ile erişebileceğine dair hesaplamalar yapılmıştır.

Önerilen erişim denetimi modeli, gerçek hayattan alınmış ve ön işlemden geçirilmiş üç farklı sektöre ait veri seti üzerine uygulanmış ve modelin performansı gerçek sistem uygulamalarında çok sık rastladığımız Rol Tabanlı Erişim Denetimi, Öznitelik Tabanlı Erişim Denetimi ve Zorunlu ve İsteği Bağlı Erişim Denetimi modellerinin performansları ile karşılaştırılmıştır. Elde edilen deneysel sonuçlar analiz edildiğinde, önerdiğimiz modelin her üç veri setinde de %90 ve üzerinde doğru erişim izni ve düzeyi sunduğu, diğer modellere kıyasla her üç sektör için de ölçeklenebilir şekilde başarılı sonuçlar verdiği test edilmiştir.

Çalışmanın ileri aşamalarında, önerilen model geliştirilerek tasarımında erişim süresini ve kullanıcının davranışlarını da esas alan yeni bir çerçeve model sunulacaktır.

KAYNAKÇA

1. Andress, J., The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier Inc., pp. 17-49, 2011.

2. Whitman, M. E. and Mattord, H. J., Principles Of Information Security, Course Technology, Cengage Learning, USA, 2012.

3. Solomon, M. G. and Kim, D., Fundamentals of Information Systems Security (3rd ed.), Jones & Bartlett Learning, 2016.

4. Güçlü, M., Bakır, Ç., Hakkoymaz, V. ve Diri, B., "Comparisons on intrusion detection and prevention systems in distributed databases,", Balkan Journal of Electrical and Computer Engineering, Vol. 7, pp. 446–455, 2019.

5. Boiko, A., Shendryk, V. and Boiko, O., "Information systems for supply chain management: uncertainties, risks and cyber security", Vol. 149, pp. 65-70, 2019.

6. Kayes, A. S. M., vd., Achieving security scalability and flexibility using Fog-Based Context-Aware Access Control, Elsevier Inc., Vol. 107, pp. 307–323, 2020.

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

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

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

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

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

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

13. Pandey, S., vd., "Security enforcement using TRBAC in cloud computing", Proceedings of the International Conference on Computing, Communication and Automation (ICCCA), IEEE, pp. 1232–1238, 2016.

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

15. Dorairaj, S. D. and Kaliannan, T., "An Adaptive Multilevel Security Framework for the Data Stored in Cloud Environment", The Scientific World Journal, 2015.

16. Huh, J. H., vd., "Next-Generation Access Control for Distributed Control Systems", IEEE Internet Computing, Vol. 20, No. 5, pp. 28-37, 2016.

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

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

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

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

21. Gunjan, B., Vijayalakshmi, A., Jaideep, V. and Shamik, S., "Deploying ABAC Policies Using RBAC Systems", Journal of Computer Security, Vol. 27, No. 4, pp. 483-506, 2019.

22. Liu, M., Yang, C., Li, H. and Zhang, Y., "An Efficient Attribute-Based Access Control (ABAC) Policy Retrieval Method Based on Attribute and Value Levels in Multimedia Networks", Sensors, Vol. 20, No. 6, 2020.

23. Xu, Y., vd., "A Feasible Fuzzy-Extended Attribute-Based Access Control Technique", Security and Communication Networks, 2018.

24. Andrews, K., Steinau, S. and Reichert, M., "Enabling Fine-Grained Access Control in Flexible Distributed Object-Aware Process Management Systems", IEEE 21st International Enterprise Distributed Object Computing Conference (EDOC), pp. 143-152, 2017.

25. Mundbrod, N. and Reicbert, M., "Object-Specific Role-Based Access Control", International Journal of Cooperative Information Systems, Vol. 28, No 1, 2019.

26. Liao, B., vd., “Security analysis of IoT devices by using mobile computing: a systematic literature review”, IEEE, Vol. 8, pp. 120331– 120350, 2020.

27. Li, M., vd., “Modelling features-based birthmarks for security of end-toend communication system”, Security and Communication Networks, Vol. 2020, 2020.

28. Zhang, J., vd., “Multicriteria decision and machine learning algorithms for component security evaluation: library-based overview”, Future of Information and Communication Conference, Vol. 2, pp. 964– 974, 2019.

29. Rains, T., Cybersecurity Threats, Malware Trends, and Strategies: Mitigate exploits, malware, phishing, and other social engineering attacks, Packt Publishing, 2020.

30. Cunningham, C., Cyber Warfare – Truth, Tactics, and Strategies: Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare, Packt Publishing, 2020.

31. Stapleton, J. J., Security without Obscurity: A Guide to Confidentiality, Authentication, and Integrity, CRC Pres, pp. 91-161, 2014.

32. Boyd C., Mathuria, A. and Stebila, D., Protocols for Authentication and Key Establishment, Springer, pp. 135-164, 2020.

33. Wilson, Y. and Hingnikar, A., Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0, Apress, pp. 159-166, 2019.

34. Braz, C., Seffah, A. and Naqvi, B., Integrating a Usable Security Protocol into User Authentication Services Design Process, CRC Pres, pp. 32-67, 2019.

35. Verma, G., Implementation of Authentication and Transaction Security: Network Security using Kerberos, Lambert Academic Publishing, 2013.

36. Saracino, A. and Mori, P., Emerging Technologies for Authorization and Authentication, ETAA 2019, Springer, pp. 86-103, 2019.

37. Boulgouris, N. V., Plataniotis, K. N. and Tzanakou E. M., Biometrics: Theory, Methods, and Applications, IEEE, pp. 633-654, 2010.

38. Hu, V. C., Ferraiolo, D. F. and Kuhn D. R., Assessment of Access Control Systems, Interagency Report 7316, NIST, pp. 11-24, 2006.

39. Chapman, N. and Chapman, J., Authentication and Authorization on the Web, MacAvon Media, 2012.

40. Fang, H., Qi, A. and Wang, X., "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement", IEEE, Vol. 34, pp. 24-29, 2020.

41. Sun, W., vd., Role-Mining Optimization with Separation-of-Duty Constraints and Security Detections for Authorizations, MDPI Future Internet, 2019.

42. Singh, G., "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975 – 8887), Vol. 67, pp. 33-38, 2013.

43. Ramesh, A. and Suruliandi, A., "Performance analysis of encryption algorithms for Information Security", 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), IEEE, pp. 840-844, 2013.

44. Zhang, D., "Big Data Security and Privacy Protection", International Journal of Computer Science and Technology, Vol. 3, pp. 35-41, 2019.

45. Xu, G., vd., "Data Security Issues in Deep Learning: Attacks, Countermeasures, and Opportunities", IEEE, Vol. 57, pp. 116-122, 2019.

46. Zhang, M., Raghunathan, A. and Jha, N. K., "A defense framework against malware and vulnerability exploits", International Journal of Information Security, Vol. 13, pp. 439-452, 2014.

47. Ye, Y., vd., "A Survey on Malware Detection Using Data Mining Techniques", ACM Computing Surveys, Vol. 50, 2017.

48. Borbely, R. C., On normalized compression distance and large malware, Journal of Computer Virology and Hacking Techniques, Springer, Vol. 12, pp. 235-242, 2016.

49. Benjamin, V., vd., "Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops", IEEE International Conference on Intelligence and Security Informatics, ISI, pp. 85-90, 2015.

50. Jouini, M., Rabai, L. B. A. and Aissa, A. B., Classification of Security Threats in Information Systems, Elsevier Inc., Vol. 32, pp. 489-496, 2014.

51. Pearce, M., Zeadally, S. and Hunt, R., "Virtualization: Issues, security threats, and solutions", ACM Computing Surveys, Vol. 45, 2013.

52. Yoo, H. and Shon, T., Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture, Elsevier Inc., Vol. 61, pp. 128-136, 2016.

53. Abomhara, M. and Køien, G. M., "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of Cyber Security and Mobility, Vol. 4, pp. 65-88, 2015.

54. Cavelty, M. D., Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities, Science and Engineering Ethics, Springer, Vol. 20, pp. 701-715, 2014.

55. Cherdantseva, Y., vd., A review of cyber security risk assessment methods for SCADA systems, Computers & Security, Elsevier Inc., Vol. 56, pp. 1-27, 2016.

56. Bojanc, R. and Blažič, B. J., "A Quantitative Model for Information-Security Risk Management", Engineering Management Journal, Vol. 25, pp. 25-37, 2013.

57. Li, Y., vd., "Anomaly Detection of User Behavior for Database Security Audit Based on OCSVM", 2016 3rd International Conference on Information Science and Control Engineering (ICISCE), IEEE, pp. 214–219, 2016.

58. Steinbart, P. J., vd., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society, Elsevier Inc., Vol. 71, pp. 15-29, 2018.

59. Benantar, M., Access Control Systems: Security, Identity Management and Trust Models, Springer, pp. 1-39, 2006.

60. Malik, A. K., Anjum, A. and Raza B., Innovative Solutions for Access Control Management, IGI Global, pp. 160-196, 2016.

61. Gabillon, A., Gallier, R. and Bruno, E., Access Controls for IoT Networks, SN Computer Science, Springer, 2020.

62. Qiu, M., vd., Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Generation Computer Systems, Elsevier Inc., Vol. 80, pp. 421-429, 2018.

63. Ferrari, E., Access Control in Data Management Systems, Morgan & Claypool Publishers, 2010.

64. Chin, S. K. and Older, S. B., Access Control, Security, and Trust: A Logical Approach, CRC Press, 2010.

65. Sahafizadeh, E. and Parsa, S., "Survey on access control models", 2nd International Conference on Future Computer and Communication, IEEE, Vol. 1, pp. 1-3, 2010.

66. Jin, X., Krishnan, R. and Sandhu, R., A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC, IFIP Annual Conference on Data and Applications Security and Privacy, Springer, pp. 41-55, 2012.

67. Bokefode, J. D., vd., "Analysis of DAC MAC RBAC Access Control based Models for Security", International Journal of Computer Applications (0975 – 8887), Vol. 104, pp. 6-13, 2014.

68. Manivannan, S. S., vd., "Multi Authority Privacy Preserving Protocol in Cloud Computing Authentication using Grouping Algorithm and EDAC-MAC", 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), IEEE, pp. 1053-1058, 2019.

69. Ferraiolo, D., Kuhn, D. R. and Chandramouli, R., Role-Based Access Control, Artech House, 2007.

70. Kim, S., vd., A feature-based approach for modeling role-based access control systems, Journal of Systems and Software, Elsevier Inc., Vol. 84, pp. 2035-2052, 2011.

71. Hu, V. C., vd., Attribute-Based Access Control, Artech House, 2017.

72. Hu, V. C., vd., "Attribute-Based Access Control", Computer, IEEE, Vol. 48, pp. 85-88, 2015.

73. Özsü, M. T. and Valduriez, P., Principles of Distributed Database Systems, Springer, 2011.

74. Stockinger, H., "Distributed Database Management Systems and the Data Grid", Eighteenth IEEE Symposium on Mass Storage Systems and Technologies, IEEE, 2001.

75. Thuraisingham, B., Multilevel security issues in distributed database management systems II, Computers & Security, Elsevier Inc., Vol. 10, pp. 727-747, 1991.

76. Larson, J. A., Database Directions: From Relational to Distributed, Multimedia and Object-Oriented Database Systems, Prentice Hall, 2017.

77. Verma, A. K. and Tamhankar, M. T., "Reliability-based optimal task-allocation in distributed-database management systems", IEEE Transactions on Reliability, Vol. 46, pp. 452-459, 1997.

78. Panahi, V. and Navimipour, N. J., "Join query optimization in the distributed database system using an artificial bee colony algorithm and genetic operators", Concurrency and Computation Practice and Experience, Vol. 31, 2019.

79. Abbas, Q., vd., "Concurrency control in distributed database system", International Conference on Computer Communication and Informatics (ICCCI), IEEE, pp. 1-4, 2016.

80. Thuraisingham, B. and Ford, W., “Security constraint processing in a multilevel secure distributed database management system”, IEEE Transactions on Knowledge and Data Engineering, Vol. 7, pp. 274-293, 1995.

81. Blaze, M., vd., The Role of Trust Management in Distributed Systems Security, Secure Internet Programming, Springer, Vol. 1603, pp. 185-210, 1999.

TEZDEN ÜRETİLMİŞ YAYINLAR

İletişim Bilgisi: mehmetguclu007@gmail.com

Makaleler

1. Guclu, M., Bakir, C. and Hakkoymaz, V., "A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security", Big Data, Scientific Programming, and Industrial Internet of Things, Scientific Programming, Vol. 2020, pp. 1-10, 2020.

2. Guclu, M., Bakir, C. and Hakkoymaz, V., "Comparisons on Intrusion Detection and Prevention Systems in Distributed Databases", Balkan Journal of Electrical and Computer Engineering, Vol. 7, No. 4, pp. 446-455, 2019.

3. Guclu, M., Bakir, C. and Hakkoymaz, V., "Intrusion Prevention Methods in Distributed Databases", Gümüşhane Fen Bilimleri Enstitüsü Dergisi, Vol. 10, No. 2, pp. 425-441, 2020.

Konferans Bildirileri

1. Guclu, M. ve Hakkoymaz, V., "Dağıtık Veritabanı Sistemleri için Güvenlik Modeli Tasarımı", 5. Ulusal Yüksek Hesaplamalı Başarım Konferansı, 2017.