Yalvaç Akademi Dergisi

https://dergipark.org.tr/tr/pub/yalvac

Öğrenci Bilgi Sistemi için Rol Tabanlı Erişim Kontrolü Yaklaşımı

Dr. Ayhan GÜLTEKİN[1*], Faruk ALTUNTAŞ[2], Zehra ALTUNTAŞ[2], Ömer Faruk GERZELİ[1]

[1] Kocaeli Üniversitesi, Öğrenci İşleri Daire Başkanlığı, Kocaeli, TÜRKİYE
[2] Kocaeli Üniversitesi, Bilgisayar Araştırma ve Uygulama Merkezi , Kocaeli, TÜRKİYE
* Sorumlu yazar : ayhan.gultekin@kocaeli.edu.tr

DOI: 10.57120/yalvac.1523803

Özet: Günümüzde, akademik kurumların iletişim gereksinimlerinin artmasıyla birlikte, Öğrenci Bilgi Sistemlerinin kullanımı vazgeçilmez bir ihtiyaç haline gelmiştir. Bu sistemler, hizmet verdikleri kullanıcı sayısının büyüklüğü nedeniyle büyük ölçekli sistemler arasında yer almakta ve bu durum sistemlerin yönetiminde önemli zorluklara yol açmaktadır. Kullanıcı sayısındaki artış, sistemlerin yükünü artırmakta, aynı zamanda kullanıcıların farklı erişim düzeylerine sahip olmaları, sistem yönetimini daha karmaşık bir hale getirmektedir. Bu bağlamda, büyük ölçekli sistemlerde kullanıcıların sisteme erişim yetkilerinin ve sistem üzerindeki izinlerinin etkin bir şekilde yönetilmesi ve planlanması, kritik bir sorun olarak ortaya çıkmaktadır. Bu sorunun çözümü için literatürde farklı yaklaşımlar kullanılmaktadır. Bu yaklaşımlardan birisi olan Rol Tabanlı Erişim Kontrolü (RBAC) yönteminin bilgi sistemlerine uygulanması ile planlamaların daha esnek ve işlevsel bir biçimde gerçekleşmesi, kullanılan yazılım kodlarının daha yalın ve modüler hale getirilmesi, uygulama bileşenlerinin daha az kod kullanılarak gereksinimlere uygun biçimde geliştirilmesi, kullanıcı arayüzlerinin daha işlevsel, yönetilebilir ve güvenli olması, ayrıca veri tabanı tasarımlarının sadeleştirilmesi sağlanabilmektedir. Bu çalışmada, Öğrenci Bilgi Sistemlerinde RBAC kullanılarak kullanıcı erişim seviyelerinin ve yetkilerinin yönetimine yönelik bir model önerilmektedir.

Anahtar Kelimeler: Bilgi Güvenliği, Öğrenci Bilgi Sistemi, Rol Tabanlı Erişim Kontrolü, Sistem Modelleme, Yetkilendirme

Role-Based Access Control Approach for Student Information System

Abstract: Recently, with the increasing communication needs of academic institutions, the use of Student Information Systems has become an indispensable necessity. These systems, due to the large number of users they serve, are classified as large-scale systems, which leads to significant challenges in their management. The increase in the number of users adds to the system's load, while the presence of users with different access levels further complicates system management. In this context, the effective management and planning of user access rights and permissions within large-scale systems emerge as critical issues. Various approaches are employed in the literature to address this issue. One such approach is the application of Role-Based Access Control (RBAC) to information systems, which enables more flexible and functional planning, simplifies and modularizes the software code used, allows the development of application components in a more efficient manner with less code, enhances the functionality, manageability, and security of user interfaces, and streamlines database designs. In this study, a model is proposed for managing user access levels and permissions in Student Information Systems using RBAC.

Keywords: Authorization, Information Security, Role Based Access Control, Student Information System, System Modelling

1. GİRİŞ

Günümüzde bilgisayarlar tek kullanıcının erişim yaptığı sistemler yerine bir de fazla kullanıcının aynı anda erişim yaptığı çok kullanıcılı sistemlerdir. Çoklu kullanıcılarının her birinin erişim yetkisine göre sistem üzerinde yetki seviyeleri farklı olabilmektedir. Web tabanlı ve mobil uygulamalardan sağlanan hizmetlerin sayısının ve çeşidinin artması aynı kaynaklar üzerinden erişim sürecinde yetkilendirme yapılmasını önemli bir zorunluluk haline getirmiştir.

Bilgi sistemlerinin büyüklük ölçeği genel olarak kullanıcı sayılarına göre belirlenir [1]. Bu sistemler çok farklı alanlarda hizmet verebilir. Sistem içerisindeki kullanıcı sayısının fazlalığı kullanılan sistemin hangi ölçüde yoğun olduğunun da temel belirleyicisidir. Büyük sistemler çok fazla sayıda kullanıcısı olan buna bağlı olarak çok fazla işlem hacmi olan sistemlerdir. Yapmış oldukları hizmet ve amaçlarına göre doküman yönetim sistemi, öğrenci bilgi sistemi, bankacılık sistemleri gibi birçok bilgi sistemi vardır. Bunların arasında bulunan öğrenci bilgi sistemleri özelleşmiş yapısı ve sunmuş oldukları hizmete göre aktif birçok kullanıcıya hizmet verir. Öğrenci bilgi sistemi içerisinde öğrenci kayıt işlemleri, akademik personel not işlemleri ve mezuniyet süreçleri gibi birçok süreç yürütülür.

Öğrenci bilgi sistemi gibi büyük ölçekli ve çok kullanıcılı sistemlerde kullanıcı yetkilerinin planlanması ve erişim yapılacak kaynaklarda yetki seviyelerinin oluşturulması önemli bir zorunluluktur. Öğrenci bilgi sisteminde birbirinden bağımsız modüller ve kullanıcı tipleri bulunur. Öğrenci işleri sorumlusunun yetkisinde olan sayfalara diğer idari personellerin erişememesi veya akademik personelin sorumluluğunda olan not verme süreçlerinin yetkisiz personelin erişimine açık olmaması gereklidir. Kurum içerisinde yeni göreve başlayan ya da mevcut görev değişikliklerinde yapılacak yetkilendirme süreçlerinin, personelin erişim yapacağı modüller ve bu modüller üzerinde yapacağı işlemlerde ekleme, güncelleme, silme bilgilerini içerecek şekilde planlanması gerekir. Veri güvenliğinin sağlanması ve erişim kontrollerinin belirlenmesi bir sistemin amacına uygun olarak hizmetlerini yerine getirmesi için oldukça önemlidir.

Erişim yönetimi, veri kaynaklarına erişim hakkı bulunan kullanıcıların belirlenmesi ve bu kullanıcıların kullanım kısıtlarının tanımlanması süreçlerinin bütünü aynı zamanda kaynağa erişim ve kullanım haklarının yetkiler verilerek ve kısıtlamalar getirilerek sınırlandırılmasıdır. Bilgi sistemlerinde işlem hacminin ve kullanıcı sayısının artması ile erişim kontrolü sadece bir seçenek olmaktan çıkıp zorunlu bir gereklilik haline gelmektedir.

Özellikle bilgi güvenliği açısından büyük öneme sahip olan erişim kontrolü, uluslararası standartlar ve yerel düzenlemelerde geniş bir şekilde ele alınmaktadır. Erişim kontrollerine ilişkin düzenlemeler içeren bazı önemli standartlar aşağıda belirtilmiştir;

1. ISO/IEC 27002:2022 Bilgi Güvenliği ve Bilgi güvenliği Kontrolleri
2. Bilgi ve İlgili Teknoloji için Kontrol Amaçları (Control Objectives for Information and Related Technology - COBIT),
3. Ödeme Kartı Sektörü Veri Güvenliği Standardı (PCI Data Security Standard - PCI DSS),
4. Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ (BDDK),
5. Ülkemizde de birçok kuruluşun uygulaması gereken Sarbanes-Oxley yasası

Belirtilen standartlardaki temel amaç veri gizliliğinin sağlanması, erişebilir kaynaklar için yetkilendirme temelli bir alt yapının oluşturulmasıdır. Ancak bu yapının oluşturulması ve işletilmesinde zorluklarda oluşabilmektedir.

Önerilen çalışmada, öğrenci bilgi sistemleri için rol tabanlı erişim kontrol yöntemi (RBAC) uygulanarak erişim ve yetkilendirme sorunlarının azaltılması için bir sistem modeli önerilmektedir. Önerilen model ile süreçlerin hızlandırılması, kullanıcı rollerinin tanımlanması ve gerektiğinde güncellenerek izinlerin merkezi bir şekilde yönetilmesi sağlanmaktadır. Böylece, karmaşık izin yapılandırmalarının etkin ve dinamik bir şekilde yönetimi önemli ölçüde kolaylaşmaktadır. RBAC ile planlama, yetkilendirme ve kod karmaşıklığı maliyetlerinin azaltılması hedeflenmektedir.

Bu çalışma giriş kısmından sonra 2.kısımda literatürde kullanılmış olan erişim kontrol yöntemlerinden, 3.kısımda Öğrenci Bilgi Sistemlerine RBAC uygulamasından ve son kısımda ise sonuçlardan oluşmaktadır.

2. ERİŞİM KONTROL YÖNTEMLERİ

Erişim yönetim modelleri için aşağıda belirtilen farklı erişim yöntemleri uygulanmaktadır;

- Zorunlu erişim kontrolü
- Öznitelik tabanlı erişim kontrolü
- Erişim kontrol listeleri
- Rol tabanlı erişim kontrolü

Zorunlu Erişim Kontrolü (Mandatory Access Control - MAC), standart olarak tanımlanmış gizlilik sınıflarını ve sınıflara erişim sağlayacak kullanıcı düzeylerini tanımlar. Her bir erişim yöntemine ait gizlilik sınıfları bulunmaktadır ve bu gizlilik sınıfları genellikle değiştirilemezler. Askeri belgelerin sınıflandırılması işleminde

kullanılan "Tasnif Dışı", "Hizmete Özel", "Gizli" ve "Çok Gizli" şeklinde tanımlanmış olan erişim sınıfları Zorunlu Erişim Kontrolü Yöntemine örnektir [2].

Öznitelik Tabanlı Erişim Kontrolü (Attribute Based Access Control - ABAC), genel olarak doğrudan kaynaklara izin atamak yerine belli nesnelere göre kullanıcı yetkilendirmesine göre modellenir. Örneğin belirli bir departman üzerinden gelen isteklere göre yetkilendirme kontrollerinin yapılması bu tip kontrollere örnektir [3]

Erişim Kontrol Listesi (Access Control List - ACL): Bir nesneyle ilişkilendirilen ve nesneye erişebilecek tüm özneleri, nesne üzerindeki haklarıyla birlikte belirten bir listedir. Listedeki her giriş özne ve haklar olmak üzere çift halinde girilir. Bir ACL, erişim kontrol matrisinin bir sütununa karşılık gelir. ACL'ler modern işletim sistemlerinde sıklıkla doğrudan ya da dolaylı olarak uygulanabilmektedir [4].

Rol Tabanlı Erişim Kontrolü (Role-Based Access Control - RBAC) bilgi işlem kaynaklarının yönetim ve işletiminde çok yaygın olarak kullanılmaktadır [5]. RBAC'de temel prensip, kullanıcıların belirli roller üzerinden yetkilendirilmesidir. Her kullanıcının bir ya da birden fazla rolü vardır ve bu rolün getirdiği izinler dâhilinde hareket edebilirler. Kullanıcının sahip olduğu rol, ona belirli izinler tanır ve bu yetkiler doğrultusunda kullanıcı sayfaları görüntüleme, verileri okuma, yazma ve silme benzeri işlemleri yapabilir [6] [7].

RBAC'de kullanıcılar doğrudan izinlere atanmaz; bu izinlerin atanması işlemi, roller aracılığıyla gerçekleştirilir. Rol, izinler ve kullanıcılar arasında bir bağlantı noktası olarak işlev görür. Kullanıcılara belirli roller atanır ve bu rollere de çeşitli izinler tanımlanır. Bu yapı sayesinde kullanıcılar, kendilerine atanmış olan roller üzerinden farklı izinler kazanabilirler [8][9]. Bir kullanıcıya ait birden fazla rol ve sahip olunan role göre farklı izinler elde edilebilir. RBAC bu sayede veri bütünlüğünü korur ve gizliliğini artırır. Çünkü kullanıcılar sahip oldukları roller ve rollere atanan izinler dolayısıyla yetkisiz erişimde bulunamamaktadır. Diğer erişim kontrol yöntemlerine kıyasla veri sızıntısı konusunda RBAC'in daha avantajlı olduğu görülmektedir [10]. Aynı zamanda sistem güvenliği ve tutarlılığı, yönetim, denetim kolaylığı ve sistemin zamanla genişlemesi durumunda ölçeklenebilir yapısı ile diğer erişim yöntemlerine göre daha avantajlıdır.

Tablo 1. Erişim Kontrol Yöntemlerinin Karşılaştırılması

Yöntem	**Referans**	**Avantaj**	**Dezavantaj**
Zorunlu Erişim Kontrolü	[2]	Yüksek Güvenlik Seviyesi	Esnek Olmaması, Yönetim Karmaşıklığı
Öznitelik Tabanlı Erişim Kontrolü	[3]	Esnek Olması, Dinamik Karar Alınabilmesi	Yönetim Karmaşıklığı, Performans
Erişim Kontrol Listeleri	[4]	Esnek Olması	Yönetim Karmaşıklığı, Performans
Rol Tabanlı Erişim Kontrolü	[5][7][8][10]	Güvenlik ve Tutarlılık, Yönetim Kolaylığı, Esnek ve Ölçeklenebilir Olması, Denetim Kolaylığı	İlk Kurulum Maliyeti, Yönetim Karmaşıklığı

3. ROL TABANLI ERİŞİM KONTROL YÖNTEMİNİN UYGULANMASI

RBAC'in temel gösterimi ve tanımlaması küme teorisi kullanarak aşağıdaki gibi yapılabilir;

- *USERS* kullanıcıların kümesi
- *ROLES* rollerin kümesi
- *OBS* kaynakların kümesi
- *OPS* işlemlerin kümesi
- $PRMS = 2^{(OBS\ X\ OPS)}$ izinlerin kümesi
- $UA \subseteq USERS\ X\ ROLES$ kullanıcı-role atamaları kümesi
- $PA \subseteq PRMS\ X\ ROLES$ kullanıcı-izin atamaları kümesi [11].

RBAC iki tür görev ayrımı tanımlamaktadır;

- Görevlerin Statik Ayrılması (SSD)
- Görevlerin Dinamik Ayrılması (DSD)

SSD, sistemdeki kullanıcı rollerinin ve bu rollerin sahip olduğu yetkilerin önceden tanımlanması ve değişken olmayan bir şekilde belirlenmesini ifade eder. Statik ayrılma, rollerin ve yetkilerin değişkenlik göstermediği

anlamına gelir. Daha basit yönetim ile güvenlik ve denetim kolaylığı sağlar ancak esneklik sorununa sahiptir. DSD ise rollerin ve yetkilerin esnek bir şekilde yönetilmesini sağlayarak organizasyon yapısının ya da kullanıcıların iş tanımının değişmesiyle güncellenebilir. Ancak SSD'ye kıyasla denetim ve yönetimi daha karmaşık olmaktadır.

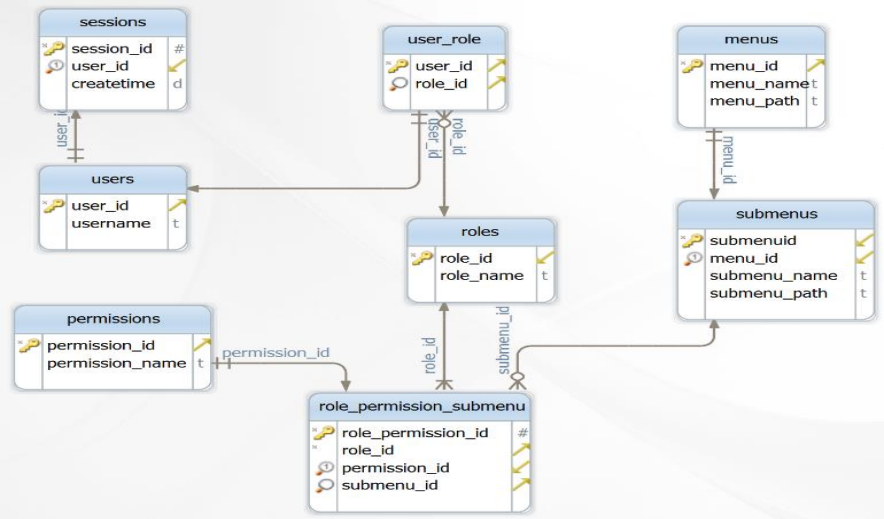
RBAC içerisinde her iki yöntem de aşağıdaki şekilde tanımlanır.

- $SSD \subseteq 2^{(ROLES)}\ X\ N^{+}$
- $DSD \subseteq 2^{(ROLES)} X\ N^{+}$

RBAC için veri tabanı içerisinde bunun için oluşturulmuş tablolar kullanılır. Bu tablolar ve bu tablolar arasındaki alanlar ve ilişkiler şekil 1'de gösterilmektedir. Önerilen modele ait veri tabanı RBAC'in yüksek bir başarımla yapılabilmesi için yalın ve işlevsel olarak tasarlanmıştır. Önerilen model uygulanması ve yönetilmesi kolay bir yapı sunmaktadır. Ayrıca esnekliğin sağlanmasını da yine veritabanında kurgulanan yapı sağlamaktadır [12].

Bu tablolarda;

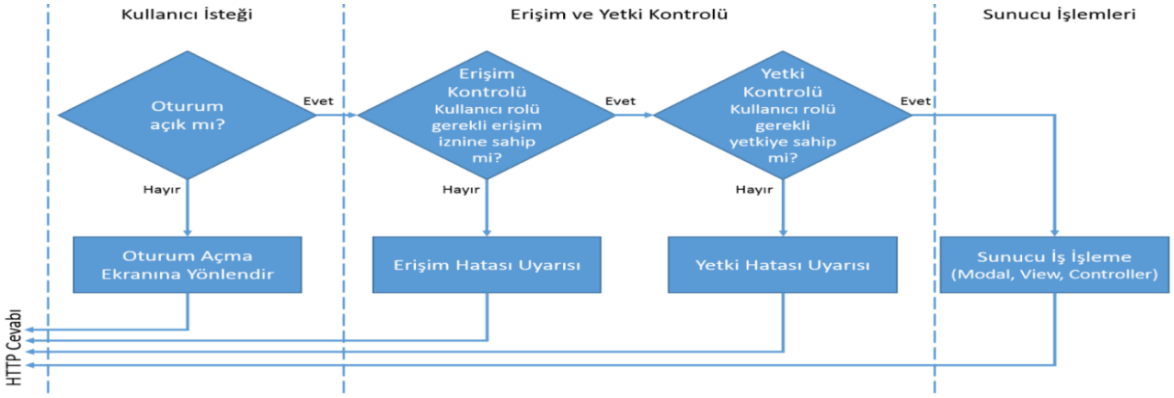
- *Sessions:* Kullanıcılara ait oturumun zaman damgası, oturum tanımlayıcısı ve benzeri bilgiler,
- *Users:* Kullanıcı hesaplarına ait isim, soyisim, parola ve benzeri bilgiler,
- *Roles:* Sistemdeki kullanıcıların sahip olabileceği rollere ait bilgiler,
- *User_Role:* Her bir kullanıcı hesabı için tanımlanmış bir veya daha fazla rol ilişkisi,
- *Permissions:* Rollerin sahip olabileceği okuma, yazma, silme ve benzeri izinler,
- *Menus:* Sistem içerisinde erişilebilecek üst menülerin bilgileri,
- *SubMenus:* Sistem içerisinde erişilebilecek alt menülerin bilgileri,
- *Role_Permission_SubMenu:* Rollerin erişebildiği alt menüler ile var olan izin ilişkileri bulunmaktadır.



Şekil 1. Veri Tabanı Tasarımı [12]

Önerilen sistemin modellenmesi esnasında sistem genel olarak şekil 2'de gösterildiği gibi 4 aşamadan oluşmaktadır. Bu aşamalar;

- Kullanıcı isteği,
- Erişim ve yetki kontrolü,
- Sunucu işlemleri
- HTTP cevabıdır.



Şekil 2. Erişim Kontrolü Akış Şeması [12]

Kullanıcı isteği, istemcilerin Öğrenci Bilgi Sistemine yaptığı HTTP isteğidir. Yapılan istek sonrası ilk olarak istekte bulunan kullanıcıya ait açık bir oturum olup olmadığı kontrol edilir. Bu kontrol session tablosu üzerinden yapılır eğer kullanıcıya ait bir oturum bilgisi mevcut değilse doğrudan oturum açma sayfasına yönlendirme yapılır. Kullanıcıya ait açık oturum bilgisi tespit edilmişse sunucu oturumun zaman aşımına uğrayıp uğramadığını kontrol eder. Bu kontrol, oturumun son aktivitesinden geçen süreye dayanarak gerçekleştirilir. Oturum süresi dolmuşsa, kullanıcı oturumu sonlandırılır ve kullanıcı oturum açma ekranına yönlendirilir. Oturum geçerli ve zaman aşımına uğramamışsa sonraki aşamada erişim ve yetki kontrolü yapılır.

Erişim ve yetki kontrolü, kullanıcıların yetkileri dahilinde hangi sayfalara erişim sağlayabilecekleri ve bu sayfalarda okuma, yazma, silme ve güncelleme yapıp yapamayacaklarını içeren bir aşamadır. Tablo 2 ve Tablo 3'de kullanıcı-rol ve rol-izin bilgileri tutulmaktadır. Erişim yetkisi role_permission_submenu tablosu üzerinden kontrol edilir. Sistem yöneticisi tam denetime sahip olup yönetici rolünden farklı olarak tüm tablolar ve veritabanı üzerinde sınırsız izne sahiptir. Bu durum dış kaynaklardan gelen tehlikelere karşı ilave koruma sağlamaktadır [13]. Kulanıcıların sayfalara erişim hakkı mevcut değilse sayfa üzerinden hata mesajı oluşturulur, kullanıcının sayfa üzerinde yetkisi var ise kullanıcı rolüne uygun olarak menus, submenus ve role_permission_submenu arasında ilişki kullanılarak ilgili menüler ekranda gösterilir. Ekrandaki menüler üzerinde işlem yapma yetkisi kod içerisinde bir parametrenin veritabanına gönderilmesi ile kontrol edilir. Veritabanında yapılan gerekli kontroller sonrasında sunucu tarafında kullanıcının yetki seviyesine uygun olarak işlem yapmasına izin verilir. Veritabanı üzerinden yapılan tüm güncellemeler, bu işlemleri yapmaya yetkili bir yönetici tarafından oluşturulan bir arayüz üzerinden kolaylıkla yapılabilmektedir. Bu arayüz üzerinden kullanıcılar seçildikten sonra bu kullanıcıların yetkili olduğu sayfalar belirlenmesi ve sonrasında bu sayfalarda hangi tür işlem yapılacağı bilgisi yine bu arayüz üzerinden yapılabilmektedir. Böylece çok daha hızlı bir şekilde yetkilendirme işlemleri tamamlanabilmektedir.

Tablo 2. Kullanıcı - Rol İlişkileri

	Roller				
Kullanıcılar	Rol_1	Rol_2	Rol_3	Rol_4	Rol_5
$Kullanıcı_1$	1				
$Kullanıc_2$		1			1
$Kullanıc_3$			1		
$Kullanıc_4$	1		1	1	
$Kullanıc_5$					1

Tablo 3. Rol - İzin İlişkileri

	İzinler				
Roller	$İzin_1$	$İzin_2$	$İzin_3$	$İzin_4$	$İzin_5$
Rol_1		1	1		
Rol_2	1				
Rol_3	1	1		1	
Rol_4			1	1	
Rol_5		1			1

Sunucu işlemleri aşamasında, erişim ve yetki kontrolü aşamasından başarıyla geçen istekler kullanıcının yetki düzeyine göre kod içerisinden veritabanına gerekli bilgiler gönderilerek alınan sonuçlara uygun olarak işletilir. Bu aşamada dikkat edilmesi gereken durum veri girişi gereken işlemlerde kullanıcı tarafından yasaklı kelime listesinde bulunan kelimelerin girişi yapılmamasıdır. Veritabanında ön tanımlı yasaklı kelime listesinin bulunması, yetkisiz kişi ya da kişilerin SQL enjeksiyonu ve benzeri müdahaleleri engellemesini sağlamaktadır [14]. Yasaklı kelime kullanılması durumunda sistem kullanıcıya hangi kelimenin yasaklı olduğunu belirten bir uyarıda bulunmaktadır. Yasaklı kelime girişi olmaması durumunda süreçte bir sonraki aşamaya geçilir.

Bu işlemler yapılırken veri değişikliklerinin kaynağını belirleyebilen kayıt sisteminin kullanılması çok önemlidir. Bir veri ihlali ya da hata durumunda, kayıt sistemi aynı zamanda sorunun kaynağını belirleyebilmekte ve oluşturma, silme ve güncelleme gibi olayları yanında olayın gerçekleştiği zamanı ve bunları gerçekleştiren kişiyi de kaydetmektedir [15].

Son aşamada, sunucunun işlediği isteğe göre bir HTTP cevabı oluşturulur ve kullanıcının tarayıcısına veya istemci uygulamasına gönderilir. HTTP cevabı istenen bilgilere, işlemin sonucuna ve işlem sırasında ortaya çıkan herhangi bir hataya dair bilgileri içerir. Daha sonra kullanıcı tarayıcısı HTTP cevabını alır ve kullanıcıya sunar. Sunucunun oluşturduğu cevap belirli bir formattadır. Bu format içerisinde başlık, gövde, durum kodu, hata bilgileri, yanıt süresi gibi bilgiler bulunur. Özellikle gövde içerisindeki bilgi asıl içeriği oluşturur. Bu içerik HTML, JSON veya XML gibi farklı formatlarda sunulabilir. Aynı zamanda sunulan cevapta resim veya farklı türde medya türleri olabilir. Durum kodları içerisinde 200 OK başarılı cevabı, 404 istenen kaynak bulunamadı veya 500 Internal Server Error gibi farklı hata kodları olabilir. Yanıt süresi ile istemcinin yaptığı bilgi talebi sonrası sunucundan cevap bilgisinin ne kadar sürede geldiği belirlenebilir.

4. SONUÇ

Bu çalışmada, RBAC yönteminin büyük ölçekli bilgi sistemlerinde kullanıcı erişim seviyelerinin belirlenmesinde ve yönetilmesinde etkili olduğu ortaya konulmuştur. Öğrenci Bilgi Sistemi modellemesinde RBAC yöntemi kullanılarak büyük ölçekli sistemlerde kullanıcı yetkilendirmelerinin tanımlanan izinlere uygun olarak yapılması sağlanmaktadır. RBAC yöntemi mevcut organizasyon yapısına uygun olarak çalışmakta ve kullanıcıların erişim sağlayacağı modüller ve bu modüller içerisinde yapacağı veri tabanı işlemleri ölçeğinde yetkilendirme yapabilmektedir. RBAC yönteminin yönetici boyutunda kullanılması yalın bir arayüz üzerinden yapılabilmektedir. Kullanıcıların arayüz üzerinden listelenmesi için LDAP (**Lightweight Directory Access Protocol**) ve benzeri alt yapılar kullanılabilmektedir. RBAC yöntemi diğer erişim yöntemlerine göre özellikle karmaşık ve hiyerarşik kullanıcı yetkilendirmelerinde esneklik sağlar, esnek ve basit yapısı ile yetkilendirme işlemleri çok kısa süre içerisinde tamamlanabilir. RBAC yöntemi tek başına çoğu zaman etkili bir çözüm sunabilse de diğer erişim yöntemleri ile kullanımı ile daha başarılı performanslar sağlanabilir ve sistemin sunduğu işlevsellik artırılabilir. Gelecekteki çalışmalarda özellikle farklı erişim yöntemlerinin birlikte kullanımı ile esneklik ve sistem güvenliği noktasında daha başarılı modeller oluşturulabilir. Ayrıca kurum ihtiyacına uygun olarak yalnızca belirli bir erişim yöntemi kullanımı yerine özelleşmiş bir yapı sunularak hem sabit hemde dinamik olarak değişen koşullarda daha etkili ve verimli erişim kontrolü sağlanabilir. Gelecek çalışmalar için öğrenci bilgi sistemleri haricindeki farklı amaçlar için kullanılan sistemlerine uygun RBAC uygulamaları modellenebilir.

KAYNAKLAR

[1] Kamu Kurum ve Kuruluşlarının Büyük Ölçekli Bilgi İşlem Birimlerinde Sözleşmeli Bilişim Personeli İstihdamına İlişkin Esas ve Usuller Hakkında Yönetmelik. (2008, 31 Aralık). T.C. Resmi Gazete, 27097.

[2] Bertin, E., Hussein, D., Sengul, C., & Frey, V. (2019). Access control in the Internet of Things: a survey of existing approaches and open research questions. *Annals of Telecommunications*, *74*(7–8), 375–388. https://doi.org/10.1007/s12243-019-00709-7

[3] Aftab, M. U., Habib, M. A., Mehmood, N., Aslam, M., & Irfan, M. (2015). Attributed role-based access control model. *Conference on Information Assurance and Cyber Security (CIACS)* https://doi.org/10.1109/ciacs.2015.7395571

[4] Hu, V. C., Ferraiolo D., & Kuhn, D. (2006). Assessment of access control systems. Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology. 11-14 https://doi.org/10.6028/NIST.IR.7316

[5] Ferraiolo, D. F., & Cugini, J. A. (1995). Role Based Access Control: Features and Motivations. *Proceedings of Computer Security Applications*, New Orleans, ABD, 241–248.

[6] Qi, H., & Diğerleri. (2016). Access Control Model Based on Role and Attribute and Its Implementation. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, China. https://doi.org/10.1109/CyberC.2016.21

[7] Göğebakan, Y. (2005). Çok Katmanlı WEB Tabanlı Uygulamalarda Yetkilendirme Problemi. *Akademik Bilişim*, Gaziantep, Türkiye.

[8] Asaf, Z., & Diğerleri. (2014). Role Based Access Control Architectural Design Issues in Large Organizations. *International Conference on Open Source Systems and Technologies (iCOSST)*, Pakistan.

[9] Oleynik, P. P. (2016). Role-Based Access Control Model as Applied to Object-Oriented Applications. *Dynamics of Systems, Mechanisms and Machine* https://doi.org/*10.1109/Dynamics.2016.7819056*

[10] Güçlü, M., Bakır, Ciğdem., & Hakkoymaz, V. (2020). A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security. Scientific Programming, Volume 20, 6-9. https://doi.org/10.1155/2020/8875069

[11] Martinez-Garcia, C., Arribas, G. N., & Borrell, J. (2011). Fuzzy Role-Based Access Control. Information Processing Letters, 483-487. https://doi.org/10.1016/j.ipl.2011.02.010

[12] Gültekin, A., Diri, S., Altuntaş, F., & Yerlikaya, Z. (2018). Rol Tabanlı Erişim Kontrolü Kullanılarak Öğrenci Bilgi Sistemi Modellenmesi, *Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi*, Kocaeli, Türkiye, 23 - 25 Kasım 2018

[13] Fahrudin, T. M. , & Al Makruf, A. Y. (2024). Design and Implementation of a Database and RBAC for Scientific and Competency Mapping Web-based Information System for Lecturers at UPN "Veteran" Jawa Timur. Nusantara Science and Technology Proceedings, 2024(41), 297-307. doi: 10.11594/nstp.2024.4148

[14] Gaur, K., Diwakar, M., Gaur, K., Singh, P., Sachdeva, T., & Pandey, N. K. (2023). SQL Injection Attacks and Prevention. https://doi.org/10.1109/iscon57294.2023.10112156

[15] Duggineni, S. (2023). Impact of controls on data integrity and information systems. *Science and Technology*, 13(2), 32-33. doi: 10.5923/j.scit.20231302.04