Özgül, M. A. ve Demirbaş Ş. (2025). Kritik Altyapıların Savunmasında Yeni Nesil Yöntemler: Siber Saldırıların Tespitinde Yapay Zekâ Uygulamaları. EMO Bilimsel Dergi, 15(3), 31-44.

Makale Türü: Derleme Makalesi
Makale Gönderilme Tarihi: 8 Aralık 2024
Makale Kabul Tarihi: 3 Temmuz 2025

Kritik Altyapıların Savunmasında Yeni Nesil Yöntemler: Siber Saldırıların Tespitinde Yapay Zekâ Uygulamaları
New Generation Methods in the Defense of Critical Infrastructures: Artificial Intelligence Applications in Detecting Cyber Attacks

Mehmet Akif Özgül[1], *Şevki Demirbaş*[2]
[1]Elektrik Elektronik Mühendisliği(TF) Bölümü, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, Türkiye, mehmet_akif_ozgul@icloud.com, 0009-0000-0625-5192
[2]Elektrik Elektronik Mühendisliği(TF) Bölümü, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, Türkiye, demirbas@gazi.edu.tr, 0000-0001-9111-684X

Öz

SCADA (Supervisory Control and Data Acquisition) sistemleri, kritik altyapıların yönetiminde önemli bir rol oynamaktadır. Bu derleme makale, SCADA sistemlerini hedef alan siber saldırıları yapay zekâ destekli yöntemlerle tespit etme potansiyelini değerlendirmek amacıyla hazırlanmıştır. Çalışmada, son yıllardaki literatür incelenerek SCADA sistemlerinin yapısı, uygulamaları ve güvenlik zafiyetleri detaylı bir şekilde ele alınmış, SCADA sistemlerine yönelik siber saldırı türleri gözden geçirilerek bu saldırıların tespitinde yapay zekâ uygulamalarının potansiyeli değerlendirilmiş ve makine öğrenmesi ve derin öğrenme algoritmalarının bu alandaki uygulamaları karşılaştırmalı olarak analiz edilmiştir. Bulgular, makine öğrenmesi algoritmalarının diğer algoritmalara kıyasla siber saldırıları tespit etmede daha geniş çapta kullanıldığını göstermektedir. Bu bulgular, geliştirilecek yapay zekâ tabanlı siber saldırı tespit modellerinin SCADA sistemlerinin güvenliğini güçlendirmede kritik bir rol oynayabileceğini ortaya koyarken aynı zamanda yeni araştırmacılar için siber saldırı tespiti alanındaki gelişmeleri daha derinlemesine incelemelerine olanak tanıyacak teknik bir rehber niteliği taşımaktadır.
Anahtar kelimeler: *Kritik altyapı, SCADA, siber güvenlik, siber saldırı, yapay zekâ ve makine öğrenmesi*

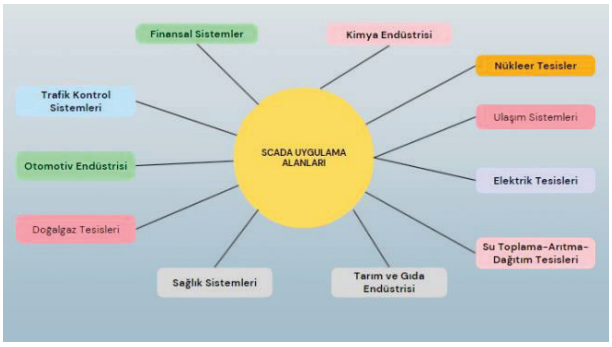
Abstract

SCADA systems play a crucial role in the management of critical infrastructures. This review article has been prepared to evaluate the potential of artificial intelligence-based methods for detecting cyber attacks targeting SCADA systems. In this study, by reviewing the literature of recent years, the structure, applications, and security vulnerabilities of SCADA systems were examined in detail; various types of cyber attacks targeting SCADA systems were analyzed; the potential of artificial intelligence applications in detecting these attacks was evaluated; and the applications of machine learning and deep learning algorithms in this domain were comparatively analyzed. The findings indicate that machine learning algorithms are more widely utilized in detecting cyber attacks compared to other algorithms. These findings reveal that the artificial intelligence-based cyber attack detection models to be developed can play a critical role in strengthening the security of SCADA systems and can also serve as a technical guide for new researchers who want to examine the developments in the field of cyber attack detection in more depth.
Keywords: *Critical infrastructure, SCADA, cyber security, cyber attack, artificial intelligence and machine learning*

1. Giriş

SCADA, elektrik üretimi, petrol, gaz ve üretim tesisleri gibi endüstriyel sektörlerde kritik altyapıların yönetiminde hayati öneme sahip bir kontrol sistemi yapısını ifade etmektedir [1]. Bu sistem, üretim tesisleri ve fabrikalar gibi kritik altyapılarda operatörlerin uzaktan erişim sağlayarak ayar noktalarını değiştirebilmesine, anahtarları ve vanaları kontrol etmelerine, alarm durumlarını takip etmelerine ve ölçüm verilerini toplayabilmelerine imkân tanımaktadır [2]. Gerçek zamanlı verilerin ve süreçlerin yerel veya uzaktan kontrolünü sağlayan SCADA sistemleri operasyonel etkinliği artırmak amacıyla sensörler, aktüatörler, anahtarlar ve vanalar gibi çeşitli bileşenleri kullanmaktadır [1]. Örneğin, belediyeler SCADA sistemlerini kullanarak şebeke suyu dağıtım tesislerindeki su tanklarının su seviyelerini, boru basınçlarını ve sıcaklıklarını izleyebilmektedir [3].

SCADA sistemleri, enerji üretimi ve dağıtımı, su ve atık su yönetimi, petrol ve gaz sektörü, kimyasal süreçler ve hatta akıllı şehirler gibi geniş bir yelpazede uygulama alanına sahip olup, bu alanlarda büyük bir öneme sahiptir (Şekil 1).



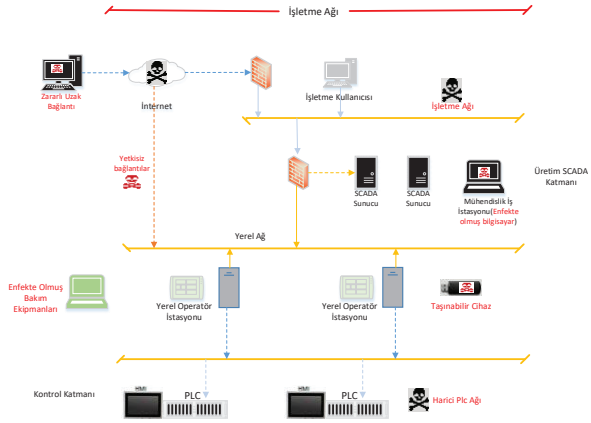
Şekil 1. SCADA sistemlerinin kullanıldığı temel uygulama alanları

Şekil 1'den de görüldüğü üzere farklı uygulama alanları bulunan SCADA sistemlerinin siber güvenliği, birçok kritik altyapı sisteminin güvenli ve kesintisiz işleyişini sağlamak için temel bir gereklilik haline gelmiş ve kuruluşların, bireylerin ve devletlerin varlıklarını koruma açısından hayati önem kazanmıştır.

Uluslararası Telekomünikasyon Birliği, siber güvenlik kavramını, bilgi ve sistemleri siber ortamda bulunan tehditlere karşı korumak için kullanılan araç, politika, kural, önlem, eylem, risk yönetimi stratejisi, eğitim, yöntem ve altyapıdan oluşan teknolojilerin bir bileşimi olarak tanımlamaktadır [4]. Siber güvenlik genel anlamda, bilgi sistemlerini ve bu sistemde barındırdıkları verileri, yetkisiz erişim, siber saldırılar ve kötü amaçlı kullanımdan korunmayı amaçlayan bir disiplindir [5].

Siber suçlular, çeşitli saldırı teknikleri ve zafiyetlerden yararlanarak özellikle kritik altyapıları kendi çıkarları doğrultusunda kullanmak için hedef almaktadırlar. Enerji, su, ulaşım, iletişim, finans, sağlık, gıda ve güvenlik kurumları gibi hayati önem arz eden temel sistemler bir ülkenin veya kurumun varlığını ve işleyişini ayakta tutan kritik altyapıları oluşturmaktadır. Bu sistemler, zorlu çalışma ortamlarına uyum sağlayabilecek ve aralıksız çalışabilecek şekilde tasarlanmış bileşenlerden oluşmaktadır. Kritik altyapıların hem yerel hem de uzaktaki bileşenlerinin izleme ve kontrol işlemleri SCADA sistemleri aracılığıyla gerçekleştirilmektedir [2].

EKS'lerde (Endüstriyel Kontrol Sistemi) bulunan SCADA ve DCS (Distributed Control System) gibi izleme ve kontrol sistemlerine yönelik gerçekleştirilen siber saldırılar, sistemlerin yetkisiz kişiler tarafından ele geçirilmesine, fonksiyonlarının ve işleyişinin bozulmasına veya değiştirilmesine neden olarak önemli güvenlik sorunları oluşturmaktadır [6]. Bu nedenle, kritik altyapılarda SCADA sistemlerinin siber saldırılara karşı korunması en yüksek önceliklerden biridir. Siber saldırılar sonucunda oluşabilecek hizmet kesintilerinin yıkıcı etkileri ve günlük yaşamın aksamasına yol açması nedeniyle SCADA sistemlerinin siber güvenliğine diğer sistemlere kıyasla daha fazla önem verilmesi gerekmektedir [7].



Şekil 2. Endüstriyel kontrol sistemlerine yönelik olası siber saldırı vektörleri

Şekil 2'de endüstriyel kontrol sistemlerine yönelik siber saldırılarda kullanılabilecek bazı yöntemler gösterilmektedir. SCADA sistemlerinde meydana gelen olayların büyük çoğunluğunda saldırganlar ve zararlı yazılımlar, sistemlere dolaylı yollarla sızmışlardır [8]. Tesis ağı ile kurumsal ağ arasında sağlanacak doğrudan bağlantılar, yetkisiz kişilerin verilere erişim sağlamasına, sistemlerde değişiklik yapmasına, kötü amaçlı yazılımlar yüklemesine veya tesis ekipmanlarını kötü amaçlarla işletmesine olanak tanıyabilmektedir. Bu tür eylemler, üretimde kesintilere neden olarak ticari kayıplara yol açabileceği gibi, en kötü senaryoda ciddi güvenlik olaylarının ortaya çıkmasına da neden olabilmektedir. Ayrıca, USB aygıtları, kasten zararlı yazılımlarla enfekte edilebilmekte ve doğrudan ya da dolaylı yollarla hedeflere ulaştırılabilmektedir. Yanlış yapılandırılmış bir güvenlik duvarı, saldırganların koruma altındaki dâhilî ağlara ve kaynaklara yetkisiz erişim elde etmesine yol açabilmektedir. Buna ek olarak tesis ağına bağlı bir PLC (Programmable Logic Controller), yeterli güvenlik önlemlerine sahip olmayan bir harici ağa bağlı olabilir ve bu durum, saldırganın tesis ağına erişim sağlamasına zemin hazırlayabilmektedir. Bu bağlantı, ciddi bir güvenlik tehdidi oluşturarak potansiyel saldırılar için zafiyet yaratabilmektedir. Bununla beraber, harici kullanılan bir dizüstü bilgisayar zararlı yazılımlarla enfekte olmuş olabilir ve işletme veya proses ağına bağlandığında bu zararlı yazılım ağı olumsuz etkileyebilir. Uzaktan destek bağlantılarının da yeterince güvenli olmaması, tesis ağını olumsuz etkileyebilmekte ve saldırganların koruma altındaki dâhilî ağlara ve kaynaklara yetkisiz erişim sağlamasına yol açabilmektedir. Bu tür siber saldırı senaryoları, Şekil 2'de gösterilen siber saldırı vektörlerinin sistemler üzerinde nasıl etkiler doğurabileceğine dair bir çerçeve sunmaktadır. Bu sistemlerin güvenlik açıklarının kapatılması ve giderilmesi, kritik altyapıların siber güvenliğini sağlamak için öncelikli adımlardan biri olmakla birlikte siber saldırıları tespit edip engellemek de en az o kadar önemlidir. Siber saldırı tespit ve engelleme sistemleri, ülkelerin kritik altyapılarının siber tehditlere karşı dayanıklılığını artırarak bu sistemlerin kesintisiz ve güvenli bir şekilde çalışmasına katkıda bulunmaktadır.

Günümüzde kritik altyapılara yapılan siber tehditlerin karmaşıklığı ve sayısı artarken büyük veri miktarları ve işlem hızı nedeniyle siber savunma için yalnızca insan odaklı yöntemler yetersiz kalmaktadır. Siber saldırıların dinamizmi ve karmaşıklığı arttıkça, geleneksel sabit algoritmalar kullanılarak yazılım geliştirmenin siber savunmada etkili bir çözüm sağlayamadığı açıkça görülmektedir [9]. Bu bağlamda, kritik altyapıların siber güvenliğini artırmak için YZ (Yapay Zekâ) tabanlı siber saldırı tespit sistemlerinin geliştirilmesi önem arz etmektedir.

Bu derleme çalışması, kritik altyapılarda siber saldırı tespiti için kullanılan yapay zekâ yöntemlerini kapsamlı bir şekilde incelemektedir. Çalışma beş bölümden oluşmaktadır. Bölüm 2, kritik altyapıların işleyişinde merkezi bir rol oynayan SCADA sistemlerine genel bir bakış sunmaktadır. Bölüm 3, SCADA sistemi uygulamaları ve sistemin güvenlik açıkları hakkında öz bilgiler vermektedir. Bölüm 4, özellikle kritik altyapılardan "Enerji" sektörüne odaklanarak SCADA sistemlerine yapılan siber saldırılardan bahsetmektedir. Bölüm 5, siber saldırıların tespiti ve bu saldırıların tespitinde yapay zekânın rolünü açıklamaktadır. Son olarak Bölüm 6'da bu araştırmanın sonuçları açıklanmaktadır.

2. SCADA Sistemi

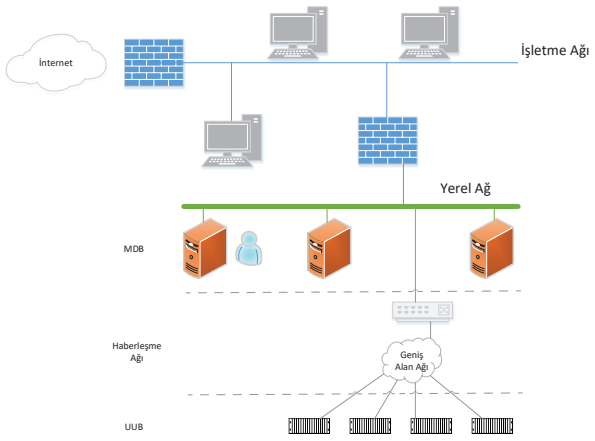
İnsanların büyük kentlere göç etmesi sonucunda şehirlerin nüfusu hızla artmış ve bu nüfus artışıyla birlikte, insanların

ihtiyaç duyduğu ışık, ısı ve enerji gibi temel gereksinimlere olan talepler de hızla artış göstermiştir. Bu artan taleplere karşılık vermek için sunulan sistemler hantal kalmış, işletmeleri yönetme, denetleme ve kontrol etme süreçleri zorlaşmıştır. Bu zorluklar karşısında SCADA sistemi bir çözüm olarak ortaya çıkmıştır.

1980'lerden beri var olan SCADA sistemi, sahadan veri toplama ve saha ekipmanlarını kontrol etme imkânı sunan, alarm bazlı izleme ve kontrol prensiplerine dayalı bir sistemdir [10]. Zamanla, SCADA sistemlerinde kullanılan PLC'lerin tedarikçileri arasında standart farklılıkları artmış, bu da iletişim problemlerine neden olmuştur. Bu sebeple, 1980'lerde bazı standartlar üzerinde anlaşmaya varılmış ve günümüzde çoğu tedarikçi, daha fazla pazar payı elde etmek amacıyla UUB'lerini (Uzak Uç Birimi) standart iletişim arayüzleri ile donatmıştır [11]. Bu sistemler, zamanla kritik altyapıların işleyişinde önemli rol oynamaya başlamıştır.

Otomasyon teknolojisi perspektifinden bakıldığında SCADA, kontrol altına alınmak istenen sistemin özel işlevlerini yerine getirebilen, fiziksel altyapılarla iletişim kurabilen ve gerekli hesaplamalar yapabilen sistemler olarak tanımlanmaktadır [2].

SCADA sistemleri, hangi operasyonel alanda kullanıldığına bakılmaksızın temel olarak Merkezi Denetleyici Birimi (MDB), uzak uç birimleri ve haberleşme ağı olmak üzere veri toplama ve kontrol işlevlerini yerine getiren üç ana bileşenden oluşmaktadır [3]. Bu temel bileşenlere ayrıca İşletme ağı da dâhil edilebilir (Şekil 3).



Şekil 3. SCADA sistemlerinin temel bileşenleri

Şekil 3'te SCADA sistemine dair temel bileşenler gösterilmektedir. Her bir bileşenin kendine has bir işlevi bulunmakla birlikte, hizmet edilen hedefe bağlı olarak bileşenlerin sayısı ve çeşitliliği değişkenlik gösterebilmektedir. MDB, sistemin durumunun anlık olarak izlendiği ve herhangi bir aksaklık veya anormallik meydana geldiğinde sisteme müdahale edilen yerdir. UUB'ler ise izlenen sistemle ilgili verileri toplar, kaydeder ve gerektiğinde bu verileri MDB'ye aktarır. MDB'ler ayrıca, verilerin kaydedilmesi ve ilgili bileşene komut gönderilmesi gibi işlevleri de gerçekleştirmektedir.

3. SCADA Sistemi Uygulamaları ve Güvenlik Zafiyetleri

Enerji santralleri, havayolları, gemi sistemleri, su arıtma tesisleri, gaz boru hatları ve demiryolları gibi kritik altyapıların işleyişini yöneten SCADA sistemleri, akademik araştırmaların odak noktasında yer almaktadır.

Endi ve arkadaşları, endüstriyel otomasyon ve proses kontrolü alanlarında kullanılmak üzere açık sistem teknolojisinden yararlanarak üç katmanlı bir SCADA sistem mimarisi sunmuşlardır. Bu mimari; denetim kontrol katmanı, proses kontrol katmanı ve saha enstrüman katmanından oluşmakta ve gerçek zamanlı bir endüstriyel süreci simule eden eksiksiz bir üç katmanlı yapıya sahiptir. Araştırmacılar, tasarladıkları açık sistem teknolojisine bağlı bu üç katmanlı mimarinin, geleneksel SCADA sistemlerinin sınırlamalarını aştığını ifade etmişlerdir [12].

Lahti ve ekibi, çeşitli web tabanlı teknolojileri otomasyon ve SCADA sistemleri açısından incelemiş ve analiz etmişlerdir. Çalışmalarında, santral otomasyonu ve SCADA sistemlerinde web kullanıcı arayüzü teknolojisinin uygunluğunu değerlendirmişlerdir. Ayrıca, enerji santrali sistem satıcıları için teknik çözümlerin temeli olarak kullanılan çeşitli web tabanlı kontrol ekranlarının son teknoloji kontrol uygulamalarına da odaklanmışlardır [13].

Chauan ve arkadaşları [14], enerji üretimi ve dağıtımı, petrol, gaz, su ve atık yönetimi gibi çeşitli sektörlerdeki kritik altyapıların kontrol ve izlenmesi için kullanılan SCADA sistemlerini incelemişlerdir. Araştırmalarında, SCADA sistemlerinin denetleyici kontrol ve veri toplama fonksiyonlarına odaklanmışlar ve dış dünyaya bireysel mesaj veya komut gönderme yeteneği olan sistemleri değerlendirmişlerdir.

İbrahim, Irak-Kerkük'te ulaştırma sektöründe kullanılan şehiriçi ve şehirlerarası yolların aydınlatma sistemini izlemek ve kontrol etmek için bir SCADA yazılımı geliştirmiştir. Çalışmasında, otomasyon ve SCADA sistemini yazılım, donanım, iletişim protokolleri ve bağlantı türleri açısından analiz etmiştir. Analizlerinin sonucunda geliştirdiği SCADA yazılımı ile aydınlatma sistemlerindeki tüm olayları izlemeyi ve kontrol etmeyi mümkün kılmıştır. Ayrıca bu yazılım ile günlük veri takibi, güvenlik ve alarm yönetimi, veri arşivi oluşturma ve raporlama gibi işlevler de sağlanmıştır. Araştırmacı, yazılımının şehir içi ve şehirlerarası yolların aydınlatma sistemlerini kontrol etmede kusursuz, senkronize ve verimli çalıştığını, aydınlatma direklerinden gelen bilgileri kullanıcılarla etkin bir şekilde paylaştığını ve aydınlatma sisteminin işletme maliyetlerini azalttığını belirtmiştir [15].

EKS/SCADA sistemleri yaygın olarak kullanılmasına rağmen sistemlerin çoğunun eski veya güncellenmemiş işletim sistemleri ve yazılım sürümleri barındırması nedeniyle güvenlik zafiyetleri bulunmaktadır. Bu durum, saldırganların güvenlik açıklarını kullanarak sisteme sızma ve kontrolü ele geçirme olasılığını artırmaktadır. SCADA sistemlerinde karşılaşılan bir başka güvenlik açığı ise standart parola güvenliği uygulamalarıdır. SCADA sistemlerinde kullanıcıların zayıf ve varsayılan parolalar kullanması yetkisiz erişime zemin hazırlamaktadır. Ek olarak, SCADA sistemleri

internete bağlı cihazlarla iletişim kurabildiğinden ve günümüzde sistemlere uzaktan erişim gibi yöntemler kullanılabildiğinden siber saldırganlar için potansiyel bir hedef hâline gelmektedir.

EKS/SCADA sistemleri günümüzde bilişim, iletişim ve internet teknolojilerinin artan kullanımıyla birlikte bilişim teknolojileriyle entegre bir şekilde çalışmaya yönelik bir eğilim göstermektedir. Bu eğilim doğrultusunda, EKS veya SCADA sistemlerinin ana bileşenleri arasında veri transferini gerçekleştirmek için özel olarak tasarlanmış haberleşme protokolleri kullanılmaktadır [16]. Amerikan Gaz Birliği'nin AGA-12 standardına göre, yaklaşık 150-200 SCADA protokolü bulunmaktadır. Modbus TCP/IP, DNP3, Ethernet/IP, Profibus ve Fieldbus en popüler ve yaygın kullanılan haberleşme protokollerindendir [17]. SCADA sistemlerinde saha cihazları ile MDB arasındaki veri iletişimini sağlayan haberleşme protokolleri, bilgi ve iletişim teknolojilerindeki güvenlik açıklarına karşı savunmasız hâle gelebilmektedir.

Haberleşme protokollerinin siber güvenlik analizleri yapıldığında, çeşitli güvenlik zafiyetlerinin olduğu bilinmektedir. Bu protokollerin güvenlik zafiyetlerinden faydalanılarak siber saldırı gerçekleştirilmesi muhtemeldir. Protokollerdeki güvenlik zafiyetlerinin sömürülmesiyle gerçekleştirilebilecek siber saldırılar amacına ve şiddetine bağlı olarak verilerin çalınması, SCADA sistemlerinin ele geçirilmesi ve devre dışı bırakılması gibi çeşitli olumsuz sonuçlara neden olabilmektedir. Örneğin, yetkilendirme ve kimlik doğrulama mekanizmalarında eksiklik bulunan protokoller çeşitli saldırılara karşı savunmasız kalmaktadır. Bu protokollerin özellikleri baz alınarak tekrarlama saldırısı, yığın tabanlı arabellek taşması, yetkisiz komut yürütme ve Dağıtılmış Hizmet Reddi (DDoS – Distributed Denial of Service) saldırısı gibi saldırılar yapılabilmektedir [18]. Bazı SCADA protokolleri, güvenlik zafiyetleri nedeniyle siber saldırılara karşı savunmasızdır. Bu tür saldırılar, endüstriyel sistemlerin verimliliğini, güvenilirliğini ve güvenliğini riske atabilmektedir.

4. SCADA Sistemlerine Yönelik Siber Saldırılar

Kritik altyapılarda kullanılan SCADA ve DCS sistemlerine yönelik gerçekleştirilen saldırılar, siber terör eylemleri olarak nitelendirilebilir [3]. Bu eylemlerin hedefleri, politik, sosyokültürel ve ekonomik boyutlarda yoğunlaşmakta ve bu alanların kesişim noktasında, tüm alanları etkileyen saldırıların özellikle kritik altyapılara yöneleceği anlaşılmaktadır [19]. Bu tür saldırılar, ekonomik dengeleri alt üst etmenin yanı sıra toplumsal hizmetlerde kesintilere yol açabilir. Bu derlemenin ilgili bölümünde, kritik altyapılar açısından büyük önem taşıyan "Enerji" sektörüne vurgu yapılmaktadır. Kritik enerji altyapısı; elektrik santralleri, iletim hatları, dağıtım şebekeleri, petrol ve doğal gaz boru hatları, depolama tesisleri ve diğer ilgili tesisler gibi enerjinin üretimi, iletimi, dağıtımı, tedariki ve depolanmasında kullanılan tüm sistemleri kapsamaktadır. Enerji sektörüne yönelik gerçekleştirilen siber saldırılar, elektrik, gaz ve ısı gibi temel hizmetlerin kesintiye uğramasına sebep olabilmektedir. Enerji kesintilerine yol açan siber saldırılar, ülkelerde toplumsal ve ekonomik istikrarı ciddi şekilde bozan kaotik bir ortam oluşturabilmektedir.

SCADA sistemleri bugüne kadar birçok siber saldırıya maruz kalmıştır. 2007, 2010 ve 2014 yıllarında farklı versiyonlarıyla ortaya çıkan BlackEnergy adlı kötü amaçlı yazılım, öncelikle DDoS saldırılarında kullanılmıştır. Son sürümünde ise, VPN (Virtual Private Network) kimliklerine erişerek şirket içi ağlarda hareket edebilir hale gelmiştir [20, 21].

2013 yılında Havex RAT adlı bir casus yazılımın birçok kritik altyapı sektöründeki endüstriyel kontrol sistemlerini hedef alan bir zararlı yazılım olarak kullanıldığı keşfedilmiştir [20, 22, 23]. Saldırganlar, kötü niyetli yazılımı SCADA sistemlerine yönelik yazılım dağıtımı yapan platformlara sızdırdılar. Bu yazılım, web sitesi üzerinden indirildikten ve kurulduktan sonra sisteme bulaşmakta ve yayıldığı kontrol ağına dâhil olan cihazlarda endüstriyel protokolleri ve portları taramaktadır.

2016 yılında Ukrayna'da gerçekleşen kötü amaçlı yazılım enjeksiyonu saldırısında zararlı yazılım, iletim trafo merkezi kontrol sistemlerine izinsiz girmiştir. Saldırı sonucunda gecenin o saatinde güç kullanımında beşte bir azalma olmuştur [24].

2016 yılı Temmuz ayında Türkiye'de enerji sektörüne yönelik gerçekleşen bir diğer önemli siber saldırı, Anonymous adlı hacker grubu tarafından İzmir Gaz firmasına karşı düzenlenmiştir. Doğal gaz dağıtım ve tedariki sağlayan firmanın internet sitesi saldırı sonrası erişime kapatılmış; kullanıcı şifreleri, faturalama bilgileri, bakım raporları ve bütçe verileri gibi kritik bilgiler ele geçirilmiştir [25].

Tablo 1, son dönemlerde dünya genelinde enerji sektörüne yönelik gerçekleştirilen çeşitli siber saldırı örneklerini sunmaktadır.

Tablo 1. Enerji sektöründe gerçekleşen önemli siber saldırılar

Ülke	Yıl	Siber Saldırı Adı	Siber Saldırı Türü	Hedef	Siber Saldırı Sonucu	Siber Saldırının Etkisi	Referans
Rusya	1982	Sibirya gaz boru hattı saldırısı	Kod manipülasyonu	Gaz boru hattı kontrol	Başarılı	3 kiloton TNT eşdeğeri patlama	Avcı [26]

				sistemi yazılımı		meydana gelmiştir.	
Litvanya	1992	Ignalia nükleer santrali siber saldırısı	Kötü amaçlı yazılım	Reaktör	Başarılı	Sistemin belirli işlevlerinde aksaklık yaşanmıştır.	Masood [27]
ABD	1999	Bellingham boru hattı felaketi	Kod manipülasyonu	SCADA sistemi	Başarılı	3 kişi öldü, birçok kişi yaralandı ve çevresel hasar meydana geldi.	Yohanandhan ve ark. [24]
ABD	2003	SQL Slammer	Kötü amaçlı yazılım enjeksiyonu	Otomasyon segmenti	Başarılı	Hizmetin kesintiye uğraması	Yadav ve ark. [28]
ABD	2007	Idaho ulusal laboratuvarı saldırısı	Yanlış veri enjeksiyonu	Dizel jeneratör	Başarılı	Dizel jeneratörün devre kesicisi manipüle edildi ve jeneratör patladı.	Yağcı ve ark. [20]
Türkiye	2008	Türkiye Petrol boru hattı saldırısı	Yanlış veri enjeksiyonu	Kontrol sistemi vanaları	Başarılı	Petrol boru hattının kontrol sistemi parametreleri manipüle edildi, petrol patlaması gerçekleşti ve 30.000 varil suda hecelendi.	Yohanandhan ve ark. [24]
İran	2010	Stuxnet	Kötü amaçlı yazılım enjeksiyonu	Santrifüjleri kontrol eden SCADA sistemi	Başarılı	Stuxnet solucanı SCADA sistemlerine sızarak santrifüjlerin normal işleyişini bozdu ve İran'da bir uranyum zenginleştirme tesisi de dâhil olmak üzere en az 14 sanayi bölgesi enfekte oldu.	Thapliyal ve ark. [29]
Katar ve Suudi Arabistan	2012	Aramco ve RasGas saldırısı	Kötü amaçlı yazılım enjeksiyonu	SCADA sistemi	Başarılı	Enerji üretimi ve dağıtımı etkilenmiştir.	Yohanandhan ve ark. [24]
Ukrayna	2015	Ukrayna Elektrik Sistemi Kesintisi	Yanlış veri enjeksiyonu	3 dağıtım şirketinde kesici ayarlarına saldırı	Başarılı	30 trafo merkezi devre dışı bırakılmış ve 230.000'den fazla kişi altı saat süreyle elektriksiz kalmıştır.	Sevim [30]
Suudi Arabistan	2017	Triton	Kötü amaçlı yazılım enjeksiyonu	Endüstriyel kontrol sistemleri	Başarılı	Kontrolörlere kötü amaçlı yazılım yüklendi ve operatörlerin erişimi engellendi.	Yağmur [31]
Dünya Geneli	2017	Dragonfly 2.0	Ağa sızma	SCADA sistemleri	Tam olarak ne kadar başarılı olunduğu bilinmiyor	Endüstriyel tesislerin üretim süreçlerini etkilemeye çalıştılar.	Yağmur [31]

ABD	2019	DDoS	Hizmet reddi	İletişim ağı	Kısmen başarılı	Kısa bir süre için elektrik sisteminin işleyişi kesintiye uğradı ancak bu bir elektrik kesintisine neden olmadı.	Yohanandhan ve ark. [24]
Hindistan	2019	Kudankulam nükleer santrali siber saldırısı	Ortadaki adam saldırısı	Santraldeki sistemler	Kısmen başarılı	Etkilenen sistemler hayati iç ağdan ayrıldı ve sistemin geri kalan işlevselliği etkilenmedi.	Yohanandhan ve ark. [24]
Rusya	2020	Bad Rabbit	Fidye yazılımı saldırısı	SCADA sistemi	Başarısız	Sisteme bulaştığında kullanıcıların dosyalarına erişimini şifreleyerek engelliyordu ancak saldırı başarıyla sonuçlanmadı. Eğer saldırı başarılı olsaydı, şirketin enerji üretim ve dağıtımını felç ederek büyük bir enerji krizine yol açabilirdi.	Yağmur [31]
ABD	2021	Colonial boru hattı saldırısı	Fidye yazılımı saldırısı	Petrol boru hattı işletim ağı	Başarılı	Şirketin sunucuları kilitlendi, ülkenin doğu yakasında benzin tedariki kesintiye uğradı. Fidye olarak 4,4 milyon dolar değerinde bitcoin ödendi.	Alomari ve ark. [32]
Ukrayna	2022	Industroyer2 saldırısı	Zararlı yazılım	Elektrik iletim ve dağıtım altyapısı	Kısmen başarılı	Planlı infaz önlenmiş olsa da, operasyonel sistemler hedef alınmış ve ülke genelinde enerji kesintisi riski oluşturmuştur.	Kozak ve ark. [33]
Danimarka	2023	Danimarka enerji altyapısı saldırısı	Güvenlik açığından yararlanma (Zyxel güvenlik duvarı zafiyeti)	22 enerji kuruluşu	Kısmen başarılı	Bilgisayar korsanları, sistemler üzerinde tam kontrol sahibi oldu. Saldırı, enerji arzını kesintiye uğratmasa da, yamalanmamış sistemlerin oluşturduğu riskleri ve kritik altyapıya önemli zarar verme	Diaba ve ark. [34]

						potansiyelini vurguladı.	
Avustralya ve Birleşik Krallık	2023	Energy One siber saldırısı	Kurumsal ağ ihlali	Energy One şirketinin Avustralya ve Birleşik Krallık' taki kurumsal sistemleri	Kısmen başarılı	Sistemlere sızma gerçekleşti. Şirket, saldırının etkisini sınırlamak için bazı sistem bağlantılarını devre dışı bıraktı ve ilgili otoriteleri bilgilendirdi. Veri sızıntısı olup olmadığı ve etkilenen unsurlar kamuoyuna açıklanmamıştır.	Diaba ve ark. [34]
ABD	2024	Halliburton saldırısı	Yetkisiz uzaktan erişim	Petrol ve doğalgaz sektörü	Başarılı	Halliburton firması operasyonel sistemlerinde yetkisiz erişim tespit etti. Bu nedenle, bazı sistemlerini devre dışı bıraktı. Finansal ve operasyonel zarar oluştu.	Kerner [35]

Tablo 1'den de anlaşılacağı üzere kritik altyapı sistemlerinde yaşanan bu tür kesintilerin etkilerinin ne kadar ciddi olduğu anlaşılmıştır. Su, elektrik, doğalgaz gibi temel hizmetlere erişimi sağlayan SCADA sistemlerinin güvenliği, milyonlarca insanın günlük yaşamını sürdürebilmesi için hayati öneme sahiptir [2]. Bu nedenlerden dolayı kritik altyapıların siber güvenliğinin sağlanması ile ilgili çalışmaların yapılması, kritik altyapıların potansiyel tehditlere karşı istikrarını ve bütünlüğünü korumak açısından elzemdir.

5. Siber Saldırı Tespitinde Yapay Zekâ Uygulamaları

SCADA sistemlerinin kritik altyapılar için oldukça maliyetli olması nedeniyle bu sistemlere yönelik siber saldırıların sebep olabileceği kesintilerin önlenmesi, hem kuruluşun hem de hizmetten yararlanan toplumun güvenliği açısından SCADA sistemlerine yönelik güvenlik tedbirlerinin alınmasını zorunlu kılmaktadır. Aslında bir bakıma, kritik altyapıların güvenliğinin sağlanması SCADA sistemlerini korumaktan geçmektedir [2].

SCADA sistemleri için gerekli önlemler alınmalı ve sistemlerin güvenliği için siber saldırı tespit sistemleri geliştirilmelidir. Siber saldırıların sıklığı ve bu saldırılardan ekonomik olarak zarar görenlerin sayısına dair net verilere ulaşmak saldırıların gizlenmesi ve suçluların yakalanmaması gibi faktörler nedeniyle zordur [36].

Literatürde siber saldırı tespiti ile ilgili çalışmalar bulunmaktadır. Angin, çalışmasında askeri otonom ağ sistemlerini siber saldırılara karşı korumaya odaklanmıştır. Angin blokzincir tabanlı bir iletişim mimarisi kullanarak veri bütünlüğü ihlalleri, kimlik doğrulama sahtekârlığı, gizli mesaj saldırıları ve ortadaki adam saldırıları gibi yaygın saldırı türlerini tespit etmeyi ve engellemeyi amaçlamıştır. Araştırmacı, bu çalışmanın veri bütünlüğü ihlalleri ve kimlik doğrulama sahtekârlığına karşı koruma sağladığını belirtmiştir [37].

Süzen ve arkadaşları [37], Endüstri 4.0'ın temel taşlarından biri olan nesnelerin kablosuz iletişiminde ağa sızma, kırma ve taklit etme yeteneklerinin veri güvenliğini nasıl etkilediğini ve bu saldırılara karşı güvenlik için hangi yöntemlerin gerektiğini değerlendirmişlerdir. Çalışmada, kablosuz ağlara ve bu ağlardaki cihazlara yönelik üç farklı saldırı senaryosu ele alınmıştır. WPA, WEB, WPA2 gibi güvenlik önlemlerinin tek başına yeterli olmadığı ve güvenlik politikaları, gizlilik, yetkilendirme ve şifreleme sistemleri gibi unsurlarla güçlendirilmesi gerektiği belirtilmiştir.

Çelik ve ark. [38], 1989 ile 2017 yılları arasında GPCoder, CryptoLocker, Winlock, Reveton, Locky, Cryptowall, Keranger, WannaCry ve Petya gibi siber saldırıları inceleyen kapsamlı bir araştırma gerçekleştirmişlerdir. Bu saldırılara karşı çözüm yöntemi olarak antispam/malware, eğitim, ağ yapısı ve yönetilmesi, yeni nesil güvenlik sistemleri, yedekleme ve veri kurtarma, operasyonel temizleme gibi bir dizi yöntem önermişlerdir.

Miciolino ve ark. [39], küçük bir şehrin su sistemini simüle eden bir siber-fiziksel test ortamında çeşitli siber saldırılar gerçekleştirerek SCADA iletişim ağının bütünlüğünü ve doğruluğunu değerlendirmişlerdir. Deneysel bulgular, endüstriyel kontrol sistemlerinde yaygın olarak kullanılan

Modbus protokolünün güvenlik açıklarını ortaya koymuştur. Araştırmacılar, bir saldırganın sistem hakkında yeterli bilgiye sahip olması durumunda, aktüatör komutlarını veya sensör okumalarını değiştirerek kötü niyetli amaçlarına ulaşabileceği sonucuna varmışlardır.

Bu ve buna benzer çalışmalar, siber saldırıların tespitinde kullanılmış olsa da, günümüzde saldırıların giderek karmaşık hale gelmesi tespit sürecini zorlaştırmıştır. Bu nedenle, güvenliği sağlamak için yazılım geliştirme öncelikli olmalı ve güçlü yasal düzenlemelerle desteklenmelidir.

Günümüzde, geleneksel saldırı tespit yöntemlerinin yerine büyük veri setlerini analiz ederek anormallikleri tanımlayabilen yapay zekâ tekniklerine yönelik eğilim artmıştır. Yapay zekânın kesin bir şekilde tanımlanması güçtür [40]. Yapay zekâ, bilgisayarlar veya dijital sistemler tarafından insan benzeri davranışları taklit eden ve belirli görevleri başarabilen bir yetenek olarak tanımlanabilir [41]. Yapay zekâ sistemlerinin bu yetenekleri kazanmasında, temelinde yatan yaklaşımlar büyük rol oynamaktadır. Bu yaklaşımların temelini yapay zekânın alt dallarından olan makine öğrenmesi ve derin öğrenme kavramları oluşturmaktadır. Bu iki kavram tamamen birbirinden bağımsız değildir ve derin öğrenme, nispeten daha yeni bir yaklaşım olarak makine öğrenmesinin bir alt kümesini temsil etmektedir [42]. Çoğu siber saldırı anlık olarak gerçekleştiği için en kısa sürede tespit edilmesi gerekmektedir. Yapay zekâ algoritmaları, büyük veri kümelerini gerçek zamanlı olarak analiz edebilir ve hızlı bir şekilde cevap verebilir.

Bununla birlikte, yapay zekâ sistemleri insan hatalarını en aza indirirken farklı türdeki siber saldırıları tanımlama ve savunma stratejileri geliştirme konusunda esneklik sağlamaktadır. Bu nedenle, yapay zekâ sistemleri siber güvenlik için kritik bir rol oynamakta olup siber saldırıları tespit etme ve engelleme konusunda temel bir araç haline gelmiştir.

Tablo 2. Siber saldırı tespitinde geleneksel yöntemler ve yapay zekâ yöntemlerinin karşılaştırılması [41,43]

Kriter	**Geleneksel Yöntemler**	**Yapay Zekâ Yöntemleri**
Tehdit tespiti	Sadece bilinen tehditleri tanır.	Bilinen ve yeni tehditleri tanıyabilir.
Uyarı ve analiz	Veriyi analiz etme ve ilişkilendirme yeteneği düşüktür.	Veriyi analiz eder, ilişkilendirir ve hızlı tepki verir.
Esneklik ve öğrenme	Dinamik tehditlere karşı esneklik gösteremez.	Öğrenerek tehditlere uyum sağlar.
Gerçek zamanlı tepki	Yalnızca tanımlı kalıpları eşzamanlı tespit eder, analiz yeteneği yoktur.	Bilinmeyen tehditleri anlık olarak tespit eder.
İnsan müdahalesi	Sürekli izleme ve manuel müdahale gerektirir.	Otomatik karar verir ve müdahale ihtiyacını azaltır.

Tablo 2, siber saldırı tespitinde kullanılan geleneksel ve yapay zekâ tabanlı yöntemleri karşılaştırarak yapay zekânın sunduğu teknik avantajları ve esneklik olanaklarını literatür ışığında özetlemektedir.

Yapay zekâ yöntemleri ile potansiyel tehditleri erken aşamada tespit edip tanımlamaya yönelik çalışmalar kritik altyapıların işleyişinde önemli bir rol oynayan SCADA sistemlerinin güvenliğini sağlamak için katkı sunabilir. Bu doğrultuda, SCADA sistemlerine yönelik çeşitli siber saldırıları önceden yüksek doğrulukla tespit edebilecek yapay zekâ tabanlı yöntemler geliştirmek büyük önem taşımaktadır.

Tablo 3'te, kritik altyapılar üzerindeki siber saldırıların yapay zekâ yöntemleriyle tespitine yönelik literatürde yer alan çalışmalar geniş bir yelpazede sunulmakta ve karşılaştırılmaktadır.

Tablo 3. Yapay zekâ yöntemleri ile siber saldırıların tespitine yönelik literatürdeki çalışmaların karşılaştırılması

Yıl	Veri Seti	Çalışmanın Amacı	Kullanılan Yöntem	Referans
2016	İçme suyu dağıtım tesisi gerçek veri seti	Siber saldırıları ve izinsiz girişleri tespit etme	Makine öğrenmesi tek sınıflı sınıflandırma	Nader ve ark. [44]
2016	Kendi oluşturdukları endüstriyel kontrol sistemleri sürece duyarlı algılama veri seti	Siber saldırıları gerçek zamanlı olarak tespit etmek	Destek vektör makinesi	Keliris ve ark. [45]
2017	Endüstri kontrol sistemi test yatağı	Anormal izinsiz giriş olaylarını tespit etme	Makine öğrenimi tabanlı bir şema	Lin ve ark. [46]
2017	Gaz boru hattı sistemi gerçek veri seti	Endüstriyel ağ paketi içeriklerinin analizini birleştiren anomalileri algılama	Bloom filtre paketi anomali algılayıcısı ve Uzun kısa süreli bellek ağ tabanlı zaman serisi düzeyi anomali algılayıcısı	Feng ve ark. [47]
2017	NSL-KDD veri seti	Endüstriyel kontrol ağlarındaki siber saldırıları tespit etme	Derin öğrenme, makine öğrenmesi	Potluri ve ark. [48]
2017	Güç sistemi saldırı veri seti	Optimizasyona dayalı olarak bir SCADA ağındaki izinsiz girişleri tespit etmek ve sınıflandırmak	İzinsiz giriş ağırlıklı parçacık tabanlı guguk kuşu arama optimizasyonu, hiyerarşik nöron mimarisi tabanlı sinir ağı	Shitharth ve Winston [49]
2017	Mississippi Eyalet Üniversitesi'nde geliştirilen bir endüstriyel kontrol sistemi veri seti	SCADA ağlarında anomali tabanlı saldırı tespiti	Makine öğrenmesi yaklaşımı kullanılarak hibrit model	Ullah ve Mahmud [50]
2018	Güvenli su arıtma test yatağı veri seti	Endüstriyel kontrol sistemlerine yönelik siber saldırıları tespit etme	Evrişimsel sinir ağları	Kravchik ve Shabtai [51]
2018	Elektrik yük tahmini veri seti	Akıllı şebekeler için siber saldırıları tespit etme	Derin öğrenme yığılmış otomatik kodlayıcı	Wang ve ark. [52]
2018	Su depolama tankı kontrol sistemi test yatağı veri seti	Su arıtma ve dağıtma süreci kontrol sistemi siber saldırıları tespit etme	Rastgele orman, karar ağacı, lojistik regresyon, Naive Bayes ve KNN algoritmaları	Teixeira ve ark. [53]
2018	Güvenli su arıtma veri seti	SCADA sistemleri tarafından kontrol edilen su şebekelerinde anomali tespiti	Lojistik regresyon, Gaussian Naive Bayes, destek vektör makinaları, KNN, karar ağacı, rastgele orman	Hindy ve ark. [54]
2018	Gaz boru hattı sisteminden toplanan gerçek veri seti	SCADA sistemlerinde izinsiz giriş tespiti	Destek vektör makinesi, rastgele orman	Perez ve ark. [55]
2019	IEC ve CyberGym SCADA laboratuvarı veri seti, Negev Ben-Gurion Üniversitesi gerçek SCADA veri seti	SCADA sisteminde tespit edilmesi zor olarak bilinen meşru işlevleri tespit etme	Zamansal örüntü tanımaya dayalı gizli markov modeli ve yapay sinir ağlarına dayalı iki algoritma	Kalech [56]

2019	KDDCup'99 veri seti	SCADA sistemlerini DDoS saldırılarına karşı korumak için 3 farklı makine öğrenimi algoritması kullanarak bir çerçeve geliştirmek	J48, Naive Bayes ve rastgele orman algoritmaları	Alhaidari ve AL-Dahasi [57]
2020	Scriptler kullanarak kendi oluşturdukları iki adet veri seti	SCADA ağları için saldırı tespit sistemi	İleri beslemeli sinir ağı, uzun kısa süreli bellek	Gao ve ark.[58]
2020	Su depolama sisteminin ağ saldırıları veri seti	SCADA ağlarındaki saldırıların belirlenmesi ve sınıflandırılması	Kümeleme, STS tabanlı geliştirilmiş guguk kuşu arama optimizasyon, genetik makine öğrenmesi tabanlı sinir ağı	Benisha ve Ratna [59]
2020	Gerçek bir trafo merkezinden elde edilen veri seti	DNP3 protokolünü kullanan SCADA sistemleri için saldırı tespit ve önleme sistemi	Denetimli ve denetimsiz makine öğrenimi algılama modelleri	Grammatikis ve ark. [60]
2020	Gaz boru hattı kontrol sistemine ait veri seti	Modbus protokolüne yönelik SCADA sistemlerine yapılan siber saldırıların analizi	Veri madenciliği, karar ağacı	Söğüt ve Erdem [16]
2021	VirusTotal ve Windows işletim sistemlerinden kendilerinin elde ettikleri veri seti	SCADA kontrollü elektrikli araç şarj istasyonunda fidye yazılımı algılama	Derin sinir ağı, 1D evrişimli sinir ağı, uzun kısa süreli bellek	Basnet ve ark[61]
2022	Gerçek zamanlı bir SCADA test yatağı veri seti	Endüstriyel process kontrol sistemleri SCADA ağında saldırı tespiti	Destek vektör makinesi, KNN, rastgele orman, NB	Rajesh ve Satyanarayana [62]
2023	WADI (Water Distribution) – Singapur Teknoloji ve Tasarım Üniversitesi	Genetik algoritma ile zenginleştirilen Naive Bayes yaklaşımı ile siber saldırıların hassas ve etkili şekilde tespiti	Genetik algoritma, NB	Tanyıldız ve ark. [63]
2024	SWaT (Secure Water Treatment) – Singapur Teknoloji ve Tasarım Üniversitesi	Endüstriyel kontrol sistemlerinde siber saldırıların sınıflandırılması	Rastgele orman, KNN, destek vektör makinesi, LSTM	Jaradat ve ark. [64]
2024	BATADAL	Su dağıtım sistemlerinde siber saldırıların tespiti	Ekstra ağaç sınıflandırıcısı ve regresyon analizi	Rustam ve ark. [65]
2025	CSE – CIC – IDS2018	IoT ortamlarında siber saldırıların tespiti	Autoencoder (AE), Deep Belief Network (DBN), Dingo Optimizer (DO)	Yarram [66]

6. Sonuçlar

SCADA sistemlerinin, enerji sektörü başta olmak üzere çeşitli endüstriyel süreçlerde geniş bir uygulama alanına sahip olmaları, bu sistemleri siber güvenlik açısından önemli bir hale getirmektedir. Yapay zekâ yöntemleri siber tehditleri gerçek zamanlı olarak tespit etmede etkili çözümler sunmaktadır. Literatürde yer alan çalışmalar, saldırı tespit sistemlerinin geliştirilmesinin önemini vurgulamaktadır. Bu derlemede, kritik altyapılardaki SCADA sistemlerine yönelik siber saldırılar ve bu saldırıların tespiti için kullanılan yapay zekâ algoritmaları son yılların literatürü ışığında incelenmiş ve karşılaştırılmıştır. Literatür taraması ve karşılaştırılmalı analiz sonucunda, siber saldırıların tespitinde makine öğrenmesi algoritmalarının diğer yöntemlere kıyasla daha yaygın bir şekilde kullanıldığı belirlenmiştir.

Literatürdeki çalışmalar, yapay zekâ yöntemlerinin kritik altyapıların siber güvenliğini sağlamak için çeşitli uygulama alanlarında kullanıldığını göstermektedir. Bu çalışmaların çoğu belirli veri kümelerine dayanmakta ve farklı yapay zekâ algoritmalarıyla gerçekleştirilmektedir. Gerçekleştirilen araştırmaların odak noktaları, yöntemleri ve uygulama yaklaşımları önemli ölçüde farklılık göstermektedir. Bazı çalışmalar daha çok algoritma temelli teknik çözümler

sunarken, bazıları uygulama bağlamına odaklanarak farklı sistemler için uyarlanabilir modeller geliştirmeyi amaçlamaktadır. Bu durum, yapay zekâ yöntemlerinin kritik altyapıların çeşitli bileşenlerine özgü şekillendiğini göstermektedir.

Bu çalışmada elde edilen bulgular, yapay zekânın siber güvenlik alanında önemli bir araç olduğunu ortaya koymaktadır. Özellikle, SCADA sistemleriyle uyumlu güvenlik çözümleri geliştirmeye odaklanan hibrit modellerin ve gelişmiş algoritmaların kullanımının artmasının kritik altyapıların siber güvenliğini güçlendirmede önemli bir rol oynayacağı anlaşılmaktadır. Bu gelişmelerin, toplumun temel hizmetlere kesintisiz erişimini sağlama açısından da kritik bir katkı sunacağı öngörülmektedir.

7. Kaynaklar

[1] A. Wali and F. Alshehry, "A survey of security challenges in cloud-based SCADA systems," *Computers,* vol. 13, no. 4, p. 97, 2024.

[2] Ş. Sağıroğlu, "Siber güvenlik ontolojisi-I," *Siber Güvenlik ve Savunma Kitap Serisi 6: Siber güvenlik ontolojisi, tehditler ve çözümler,* Nobel Akademik Yayıncılık, Ankara, 2021.

[3] E. Söğüt, "SCADA sistemlerine yönelik siber saldırıların tespiti için yeni bir hibrit makine öğrenmesi yöntemi," Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2023.

[4] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Computers & Security,* vol. 38, pp. 97-102, 2013.

[5] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future generation computer systems,* vol. 92, pp. 178-188, 2019.

[6] E. Irmak ve İ. Erkek, "Endüstriyel kontrol sistemleri ve SCADA uygulamalarının siber güvenliği: Modbus TCP protokolü örneği," *Gazi University Journal of Science Part C: Design and Technology,* vol. 6, no. 1, pp. 1-16, 2018.

[7] L. A. Maglaras *et al.*, "Cyber security of critical infrastructures," *Ict Express,* vol. 4, no. 1, pp. 42-45, 2018.

[8] E. J. Byres and P. Eng, "Cyber security and the pipeline control system," *Pipeline & Gas Journal,* vol. 236, no. 2, pp. 58-59, 2009.

[9] E. Şeker, "Yapay zeka tekniklerinin/uygulamalarının siber savunmada kullanımı," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* vol. 6, no. 2, pp. 108-115, 2020.

[10] M. Karaçor ve K. Keleş, "Otomasyon sistemlerinin bileşenleri," *VI. Otomasyon Sempozyumu, Samsun,* 2007.

[11] S. Dransfeld, "Measurement and supervision in automated production," Thesis for the Degree of Doktor Ingenior, Norwegian University of Science and Technology Faculty of Engineering Science & Technology, Trondheim. 2007.

[12] M. Endi and Y. Elhalwagy, "Three-layer PLC/SCADA system architecture in process automation and data monitoring," in *2010 the 2nd international conference on computer and automation engineering (ICCAE)*, 2010, vol. 2. pp. 774-779.

[13] J. P. Lahti, A. Shamsuzzoha, and T. Kankaanpää, "Web-based technologies in power plant automation and SCADA systems: A review and evaluation," in *2011 IEEE International Conference on Control System, Computing and Engineering*, IEEE, 2011, pp. 279-284.

[14] R. K. Chauhan, M. Dewal, and K. Chauhan, "Intelligent SCADA system," *International Journal on power system optimization and Control,* vol. 2, no. 1, pp. 143-149, 2010.

[15] M. H. İbrahim, "SCADA Sistemi: Şehir İçi ve Şehirlerarası Yolların Aydınlatma Sisteminin Kontrolü ve Otomasyonu," *Çukurova Üniversitesi Mühendislik Fakültesi Dergisi,* vol. 37, no. 3, pp. 653-662, 2022.

[16] E. Söğüt ve O. A. Erdem, "Endüstriyel kontrol sistemlerine (SCADA) yönelik siber terör saldırı analizi," *Politeknik Dergisi,* vol. 23, no. 2, pp. 557-566, 2020.

[17] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *computers & security,* vol. 25, no. 7, pp. 498-506, 2006.

[18] P. Kamal, A. Abuhussein, and S. Shiva, "Identifying and scoring vulnerability in SCADA environments," in *Future Technologies Conference (FTC)*, 2017, vol. 2017, pp. 845-857.

[19] E. Kıran ve İ. Soğukpınar, "Kritik Altyapılarda Siber Risk Analizi ve Yönetimi," *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi,* vol. 14, no. 1, pp. 15-33, 2021.

[20] M. Y. Yağci, "SCADA sistemler için güvenli model oluşturulması," Yüksek Lisans Tezi, İstanbul Üniversitesi-Cerrahpaşa Lisansüstü Eğitim Enstitüsü, 2020.

[21] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid," in *4th International Symposium for ICS & SCADA Cyber Security Research 2016*, BCS, 2016, pp. 53-63.

[22] S. Abe, Y. Tanaka, Y. Uchida, and S. Horata, "Tracking attack sources based on traceback honeypot for ICS network," in *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, IEEE, 2017, pp. 717-723.

[23] S. Abe, Y. Tanaka, Y. Uchida, and S. Horata, "Developing deception network system with traceback honeypot in ICS network," *SICE Journal of Control, Measurement, and System Integration,* vol. 11, no. 4, pp. 372-379, 2018.

[24] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid–Part–I: Background on CPPS and necessity of CPPS testbeds," *International Journal of Electrical Power & Energy Systems,* vol. 136, p. 107718, 2022.

[25] S. Akçalı ve M. B. K. Önaçan, "Türkiye'de siber saldiri olaylari ve siber savunma yeteneklerinin gelişimi," *The Journal of Academic Social Science Studies,* no. 78, pp. 351-369, 2024.

[26] İ. Avcı, "Akıllı doğal gaz şebekelerinde siber güvenlik açıklarının araştırılması ve olgunluk modeli geliştirilmesi," Doktora Tezi, İstanbul Üniversitesi Cerrahpaşa Lisansüstü Eğitim Enstitüsü, İstanbul, 2021.

[27] R. Masood, "Assessment of cyber security challenges in nuclear power plants security incidents, threats, and initiatives," *Cybersecurity and Privacy Research Institute the George Washington University,* 2016.

[28] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *International Journal of Critical Infrastructure Protection,* vol. 34, p. 100433, 2021.

[29] N. Thapliyal and S. Dhariwal, "Protecting A Nuclear Power Plant Against A Stuxnet Attack: Power Of Computer Security," in *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, 2023: IEEE, pp. 598-603.

[30] C. Sevim, "Yeni Enerji Jeopolitiğine Genel Bakış," *İzmir Sosyal Bilimler Dergisi,* vol. 2, no. 2, pp. 57-63, 2020.

[31] E. Yağmur, "SCADA sistemlerinde dagitik hizmet disi birakma saldirilarinin derin ögrenme ve makine ögrenmesi yöntemleri ile tespiti," Yüksek Lisans Tezi, Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü, Konya, 2023.

[32] M. A. Alomari *et al.*, "Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions," *Energies,* vol. 18, no. 1, p. 141, 2025.

[33] P. Kozak, I. Klaban, and T. Šlajs, "Industroyer cyber-attacks on Ukraine's critical infrastructure," in *2023 International Conference on Military Technologies (ICMT)*, 2023: IEEE, pp. 1-6.

[34] S. Y. Diaba, M. Shafie-khah, and M. Elmusrati, "Cyber-physical attack and the future energy systems: A review," *Energy Reports,* vol. 12, pp. 2914-2932, 2024.

[35] S. M. Kerner. "Halliburton cyberattack explained: What happened?" TechTarget. https://www.techtarget.com/whatis/feature/Halliburton-cyberattack-explained-What-happened (accessed 17 May, 2025).

[36] C. Hatipoğlu ve T. Tunacan, "Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması," *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi,* vol. 8, no. 1, pp. 430-445, 2021.

[37] A. A. Süzen, M. A. Şimşek, K. Kayaalp, ve R. Gürfidan, "Endüstri 4.0'da Nesnelerin Kablosuz Etki Alanlarına Yapılan Saldırı Metodolojisi," *Nevşehir Bilim ve Teknoloji Dergisi,* vol. 8, pp. 143-151, 2019.

[38] S. Çelik ve B. Çeliktaş, "Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar," *CyberPolitik Journal,* vol. 3, no. 5, pp. 105-132, 2018.

[39] E. E. Miciolino, G. Bernieri, F. Pascucci, and R. Setola, "Communications network analysis in a SCADA system testbed under cyber-attacks," in *2015 23rd Telecommunications Forum Telfor (TELFOR)*, 2015: IEEE, pp. 341-344.

[40] X. Du-Harpur, F. Watt, N. Luscombe, and M. Lynch, "What is AI? Applications of artificial intelligence to dermatology," *British Journal of Dermatology,* vol. 183, no. 3, pp. 423-430, 2020.

[41] M. M. Mijwil, E. Sadıkoğlu, E. Cengiz, ve H. Candan, "Siber güvenlikte yapay zekanın rolü ve önemi: bir derleme," *Veri Bilimi,* vol. 5, no. 2, pp. 97-105, 2022.

[42] U. Altınmakas, "Üretken Yapay Zekâ Tarafından Üretilen Fikri Ürünlerde Yapay Zekânın Eser Sahipliği ve Telif Hakkı," *Anadolu Üniversitesi Hukuk Fakültesi Dergisi,* vol. 11, no. 1, pp. 457-480, 2025.

[43] E. Şeker, "Yapay Zekâ Tekniklerinin/Uygulamalarının Siber Savunmada Kullanımı," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* vol. 6, no. 2, pp. 108-115, 2020.

[44] P. Nader, P. Honeine, and P. Beauseroy, "Detection of cyberattacks in a water distribution system using machine learning techniques," in *2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, 2016: IEEE, pp. 25-30.

[45] A. Keliris, H. Salehghaffari, B. Cairl, P. Krishnamurthy, M. Maniatakos, and F. Khorrami, "Machine learning-based defense against process-aware attacks on industrial control systems," in *2016 IEEE International Test Conference (ITC)*, 2016: IEEE, pp. 1-10.

[46] C.-T. Lin, S.-L. Wu, and M.-L. Lee, "Cyber attack and defense on industry control systems," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017: IEEE, pp. 524-526.

[47] C. Feng, T. Li, and D. Chana, "Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017: IEEE, pp. 261-272.

[48] S. Potluri, N. F. Henry, and C. Diedrich, "Evaluation of hybrid deep learning techniques for ensuring security in networked control systems," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2017: IEEE, pp. 1-8.

[49] S. Shitharth, "An enhanced optimization based algorithm for intrusion detection in SCADA network," *Computers & Security,* vol. 70, pp. 16-26, 2017.

[50] I. Ullah and Q. H. Mahmoud, "A hybrid model for anomaly-based intrusion detection in SCADA networks," in *2017 IEEE International Conference on Big Data (Big Data)*, 2017: IEEE, pp. 2160-2167.

[51] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proceedings of the 2018 workshop on cyber-physical systems security and privacy*, 2018, pp. 72-83.

[52] H. Wang *et al.*, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 11, pp. 4766-4778, 2018.

[53] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Future Internet,* vol. 10, no. 8, p. 76, 2018.

[54] H. Hindy, D. Brosset, E. Bayne, A. Seeam, and X. Bellekens, "Improving SIEM for critical SCADA water infrastructures using machine learning," in *International Workshop on Security and Privacy Requirements Engineering*, 2018: Springer, pp. 3-19.

[55] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, "Machine learning for reliable network attack detection in SCADA systems," in *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 633-638.

[56] M. Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques," *Computers & Security,* vol. 84, pp. 225-238, 2019.

[57] F. A. Alhaidari and E. M. Al-Dahasi, "New approach to determine DDoS attack patterns on SCADA system using machine learning," in *2019 International conference on computer and information sciences (ICCIS)*, 2019: IEEE, pp. 1-6.

[58] J. Gao *et al.*, "Omni SCADA intrusion detection using deep learning algorithms," *IEEE Internet of Things Journal,* vol. 8, no. 2, pp. 951-961, 2020.

[59] D. S. R. R. R.B. Benisha, "Detection of Intruison using Enhanced Machine Learning Model in SCADA Wireless Network," *International Journal of Future Generation Communication and Networking,* Research vol. 13, no. 1, 1, pp. 85-98, 2020.

[60] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.-A. Karypidis, and A. Sarigiannidis, "DIDEROT: An intrusion detection and prevention system for DNP3-based SCADA systems," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1-8.

[61] M. Basnet, S. Poudyal, M. H. Ali, and D. Dasgupta, "Ransomware detection using deep learning in the SCADA system of electric vehicle charging station," in *2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America)*, 2021: IEEE, pp. 1-5.

[62] L. Rajesh and P. Satyanarayana, "Evaluation of machine learning algorithms for detection of malicious traffic in scada network," *Journal of Electrical Engineering & Technology,* vol. 17, no. 2, pp. 913-928, 2022.

[63] H. Tanyıldız, C. B. Şahin, and Ö. B. Dinler, "Effective Cyber Attack Detection Based on Augmented Genetic Algorithm with Naive Bayes," *NATURENGS,* vol. 4, no. 2, pp. 30-35, 2023.

[64] S. Jaradat, M. M. Komol, M. Elhenawy, and N. Dong, "Cyberattack detection on SWaT plant industrial control systems using machine learning," *Artif. Intell. Auto. Syst,* 2024.

[65] F. Rustam, M. Salauddin, U. Saeed, and A. D. Jurcut, "Dual-Approach Machine Learning for Robust Cyber-Attack Detection in Water Distribution System," in *Proceedings of the 14th International Conference on the Internet of Things*, 2024, pp. 248-254.

[66] S. Yarram, "An Optimized Deep Learning Approach for Intrusion Detection: AE-DBN Hybrid Model with Dingo Feature Selection on CSE-CIC-IDS2018," in *2025 International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF)*, 2025: IEEE, pp. 1-9.

Özgeçmişler

Mehmet Akif ÖZGÜL, Karadeniz Teknik Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü'nden 2015 yılında lisans derecesi ile mezun olmuştur. Ayrıca Anadolu Üniversitesi İşletme Bölümü'nü 2020 yılında bitirmiş ve 2025 yılında Gazi Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda yüksek lisans eğitimini tamamlamıştır. 2017–2018 yılları arasında San-El Mühendislik'te saha mühendisi olarak altyapı ve enerji projelerinde görev almış, 2018'de Atlas Yapı Denetim'de kontrol mühendisi olarak çeşitli binaların elektrik projelerinin denetiminde çalışmıştır. 2018–2019 döneminde Torunlar GYO'da teknik müdür olarak enerji yönetimi, bakım-onarım süreçleri ve teknik ekiplerin koordinasyonundan sorumlu olmuştur.
2019 yılından itibaren Elektrik Üretim A.Ş. (EÜAŞ) Genel Müdürlüğü'nde görev yapmakta olup; bilgi güvenliği yönetim sistemleri, SCADA ve otomasyon güvenliği, OT güvenliği, siber güvenlik operasyonları, penetrasyon testleri ve iletişim altyapısı projelerinde yer almıştır. 2023 yılından bu yana Başmühendis – OT & Siber Güvenlik unvanıyla çalışmalarına devam etmektedir.
Araştırma ve uzmanlık alanları arasında endüstriyel kontrol sistemleri, SCADA ve OT güvenliği, bilgi güvenliği yönetim sistemleri, yapay zekâ tabanlı siber saldırı tespit yöntemleri ve kritik altyapıların korunması yer almaktadır. Bu konularda çeşitli projelerde görev almış ve ulusal/uluslararası yayınlar gerçekleştirmiştir.

Şevki DEMİRBAŞ, Lisans Eğitimini 1993 yılında Gazi Üniversitesi Teknik Eğitim Fakültesi Elektrik Öğretmenliğinde tamamlamıştır. Yüksek Lisans ve Doktora eğitimlerini sırası ile 1996 ve 2001 yıllarında Gazi Üniversitesi Fen Bilimleri Enstitüsü Elektrik Eğitimi alanında tamamlamıştır. 1994 – 1998 yılları arasında Gazi Üniversitesi Teknik Eğitim Fakültesi'nde Araştırma Görevlisi, 1998 – 2002 tarihleri arasında Öğretim Görevlisi, 2002 – 2011 tarihleri arasında Yardımcı Doçent olarak görev yapmıştır. 2011'de Doçent ünvanı almış, 2011 – 2017 tarihleri arasında Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği bölümünde doçent olarak görev yapmıştır. 2017 yılından itibaren aynı bölümde Profesör olarak görev yapmaktadır.