CYBERSECURITY IN IOT SYSTEMS FOR THE TRANSPORTATION SECTOR: THREATS, ATTACKS, AND PROTECTION STRATEGIES

YUNUS EMRE SEYYAR

ABSTRACT

The transportation sector represents a critical infrastructural element within the global economy and has experienced a significant paradigm shift in recent years, predominantly catalyzed by the rapid advancement of digital technologies. This transformation is most pronounced in the extensive integration of Internet of Things (IoT) technologies, which have substantively augmented the operational efficiency, safety standards, and environmental sustainability of transportation systems. Key applications of IoT, ranging from advanced traffic management systems and electric vehicle charging networks to the deployment of autonomous vehicles and smart passenger transportation solutions, are fundamentally redefining the operational dynamics of the sector. However, the rapid expansion of IoT-based infrastructure has concurrently introduced a wide array of cybersecurity vulnerabilities, rendering the sector increasingly susceptible to cyberattacks. These threats pose substantial economic, operational, and safety-related risks. This paper provides a systematic analysis of cyberattacks targeting Internet of Things (IoT) devices in the transportation sector. It assesses the operational and security-related implications of such threats and proposes a set of integrated cybersecurity strategies and policy-level recommendations aimed at enhancing the resilience of transportation infrastructures against these evolving attack threats.

Keywords: Transportation Sector, Cybersecurity, Internet of Things, Artificial Intelligence, Cyberattacks

Dr., Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
Mail: yunusemre.seyyar@gmail.com
ORCID: https://orcid.org/ 0000-0001-5767-8515

Makale Atıf Bilgisi:	Seyyar, Y., E. (2025). "Ulaşım Sektöründe IoT Sistemleri ve Siber Güvenlik: Tehditler, Saldırılar ve Korunma Yöntemleri". *Ulaştırma ve Altyapı,* Yıl: 2, Sayı: 2, s. (14-33)
Makale Türü:	Araştırma
Geliş Tarihi:	14.04.2025
Kabul Tarihi:	16.06.2025
Yayın Tarihi:	25.06.2025
Yayın Sezonu:	Ocak-Haziran 2025

ULAŞIM SEKTÖRÜNDE IOT SİSTEMLERİ VE SİBER GÜVENLİK: TEHDİTLER, SALDIRILAR VE KORUNMA YÖNTEMLERİ

YUNUS EMRE SEYYAR

ÖZ

Ulaşım sektörü, küresel ekonominin kritik altyapı unsurlarından birini temsil etmekte olup son yıllarda dijital teknolojilerin hızlı gelişimiyle birlikte önemli bir paradigma değişimi yaşamaktadır. Bu dönüşüm özellikle Nesnelerin İnterneti (IoT) teknolojilerinin yaygın entegrasyonu ile belirginleşmiş; bu teknolojiler, ulaşım sistemlerinin operasyonel verimliliğini, güvenlik standartlarını ve çevresel sürdürülebilirliğini önemli ölçüde artırmıştır. Gelişmiş trafik yönetim sistemlerinden elektrikli araç şarj ağlarına, otonom araçların kullanımından akıllı yolcu taşıma çözümlerine kadar uzanan IoT uygulamaları, sektörün işleyiş dinamiklerini köklü bir şekilde yeniden tanımlamaktadır. Ancak IoT tabanlı altyapının hızla yaygınlaşması, beraberinde çok sayıda siber güvenlik açığını da getirmiş ve sektörü siber saldırılara karşı giderek daha savunmasız hâle getirmiştir. Bu tehditler ekonomik, operasyonel ve güvenlik açısından ciddi riskler oluşturmaktadır. Bu çalışma ulaşım sektöründe Nesnelerin İnterneti (IoT) cihazlarını hedef alan siber saldırıların sistematik bir analizini sunmakta; bu tehditlerin operasyonel ve güvenlik odaklı etkilerini değerlendirmekte ve ulaşım altyapılarının bu evrilen saldırı tehditlerine karşı dayanıklılığını artırmaya yönelik entegre siber güvenlik stratejileri ile politika düzeyinde öneriler ortaya koymaktadır.

Anahtar Kelimeler: Ulaştırma Sektörü, Siber Güvenlik, Nesnelerin İnterneti, Yapay Zekâ, Siber Saldırılar

1. Giriş

Ulaşım sektörü küresel ekonomik büyüme ve toplumsal gelişim açısından kritik bir rol oynamaktadır. İnsan hareketliliğinin sağlanması, ticaretin etkin işlemesi ve lojistik süreçlerinin verimli yönetilmesi, ulaşımın sürdürülebilirliğine ve güvenliğine bağlıdır. Ancak artan kentleşme, nüfus yoğunluğu ve çevresel sorunlar, geleneksel ulaşım sistemlerini zorlamaktadır. Dijital teknolojiler, ulaşım sektörünün verimliliğini artırırken aynı zamanda daha güvenli ve sürdürülebilir çözümler sunmaktadır.

Akıllı Ulaşım Sistemleri (AUS); T.C. Ulaştırma Altyapı Bakanlığı sitesinde seyahat sürelerinin azaltılması, trafik güvenliğinin artırılması, mevcut yol kapasitelerinin verimli kullanılması, hareketliliğin artırılması, enerjinin verimli kullanılması ve çevreye verilen zararın azaltılması gibi amaçlar doğrultusunda geliştirilen kullanıcı, araç, altyapı ve merkez arasında çok yönlü veri alışverişi ile izleme, ölçme, analiz ve kontrol mekanizmalarını içeren bilgi iletişim temelli sistemleri olarak tanımlanmış ve Şekil 1.'de gösterilmiştir.

Şekil 1: Akıllı Ulaşım Sistemlerinin Tanımı
(Kaynak: https://hgm.uab.gov.tr/akilli-ulasim-sistemleri-aus/14.03.2025)

Ticaretin etkin işlemesi ve lojistik süreçlerinin verimli yönetilmesi, ulaşım sistemlerinin sürdürülebilirliği ve güvenliği ile doğrudan ilişkilidir (Önder & Akdemir, 2020).

Son yıllarda nesnelerin interneti (IoT), yapay zeka (AI), büyük veri analitiği, otonom araçlar ve akıllı ulaşım sistemleri, ulaşım sektöründe devrim niteliğinde dönüşümlere yol açmıştır (Macit, 2024).

IoT cihazları, trafik akışının izlenmesi, araçların konum takibi, akıllı park yönetimi ve elektrikli araç şarj istasyonları gibi uygulamalar ile ulaşım süreçlerini optimize etmektedir. Bu sayede, yolculuk süreleri kısalırken yakıt tüketimi ve trafik yoğunluğu gibi sorunlar da minimize edilebilmektedir. Ek olarak yapay zekâ destekli sistemler, gerçek zamanlı veri analizi ile trafik yönetimini daha

dinamik hale getirerek ulaşım güvenliğini artırmaktadır. Ancak, her yeni teknolojinin sunduğu avantajların yanında güvenlik zafiyetlerini de beraberinde getirdiği unutulmamalıdır. Ulaşımın dijitalleşmesi, verimliliği ve güvenliği artırırken aynı zamanda siber tehditlere karşı yeni bir savunma ihtiyacını da doğurmaktadır.

Yapay zekâ ulaşım sektöründe köklü değişiklikler yaratırken, bu teknolojilerin entegrasyonu aynı zamanda yeni siber güvenlik risklerini de beraberinde getirmektedir. YZ'nin entegrasyonu, özellikle otonom araçlar, akıllı trafik yönetim sistemleri ve talep odaklı ulaşım hizmetleri gibi alanlarda belirginleşmektedir. Bu araçlar sürücüsüz ulaşım imkânı sunarak trafik kazalarını azaltma, yakıt verimliliğini artırma ve yolculuk sürelerini optimize etme potansiyeline sahiptir. Ayrıca bu sistemleri gerçek zamanlı verileri analiz ederek trafik akışını düzenler ve tıkanıklıkları minimize eder, bu da hem zaman kaybını hem de çevresel etkileri azaltır. Talep odaklı ulaşım sistemleri ise kullanıcıların tercihlerine göre en uygun güzergahları ve araçları belirleyerek, toplu taşıma sistemlerinin daha verimli hale gelmesine katkıda bulunur. Tüm bu uygulamalar, ulaşım sistemlerinin güvenliğini ve verimliliğini artırmaktadır. Bununla birlikte bu dijitalleşmiş altyapının ve gelişmiş yapay zekâ sistemlerinin savunmasız kalması, siber güvenlik tehditlerine karşı ciddi bir açık yaratmaktadır.

Fidye yazılımı, Dağıtık hizmet reddi saldırıları, Kimlik avı ve Küresel konumlandırma sistemi (GPS) sahtekarlığı gibi tehditler, ulaşım altyapısının bütünlüğünü riske atmaktadır. Özellikle IoT cihazları ve otonom sistemler, bu saldırılara karşı korunmazsa, bireysel ve toplumsal güvenlik ciddi tehlikelerle karşı karşıya kalabilmektedir (Eleimat & Őszi, 2025).

Ulaşım sektöründeki YZ uygulamalarının verimli ve güvenli bir şekilde işleyebilmesi için siber güvenlik protokollerinin güçlendirilmesi, şifreleme teknolojilerinin ve yapay zekâ tabanlı tehdit tespit sistemlerinin etkin bir şekilde kullanılması gereklidir. YZ'nin sağladığı fırsatlar yalnızca teknolojik yenilik değil, aynı zamanda yüksek seviyede güvenlik önlemleri gerektiren bir çevreyi de beraberinde getirmektedir.

Özellikle IoT cihazlarının ve otonom sistemlerin siber saldırılara karşı korunması hem bireysel hem de toplumsal güvenlik açısından büyük önem taşımaktadır. Bu dönüşüm süreci yalnızca teknik gelişmelerin değil, aynı zamanda kapsamlı bir siber güvenlik vizyonunun da ulaşım politikalarına entegre edilmesini gerekli kılmaktadır.

Siber güvenlik olgusu yalnızca savunma önlemleri bağlamında değil, aynı zamanda siber güvensizlik kavramı üzerinden bir ölçüt olarak ele alınmakta; sektörel risklerin kapsamı ve yönetilebilirliği bu metrikle analiz edilmektedir. Siber güvensizlik terimi özellikle 2000'li yılların başından itibaren akademik literatürde kendine yer bulmuş ve devletlerin, şirketlerin ve kritik altyapıların dijital tehditlere karşı duyarlılığını tanımlamak için kullanılmaktadır (Neutze J., 2013).

Bu çalışma ulaşım sektörünün dijitalleşme sürecini ve beraberinde gelen siber güvenlik tehditlerini inceleyerek, bu tehditlere karşı alınması gereken önlemleri analiz etmektedir. Aynı zamanda, IoT sistemleri başta olmak üzere, ulaşım altyapısında

siber güvenliği sağlamaya yönelik politika önerileri ve teknolojik savunma stratejileri ele alınmaktadır. Dijitalleşen ulaşım sektörü gelecekte şehirlerin yapısını, lojistik süreçlerini ve küresel ticareti dönüştürecek bir potansiyele sahip olup bu dönüşümün güvenli ve sürdürülebilir olması için gerekli önlemlerin alınması zorunludur.

Sıkça kullanılan kısaltmalar, Türkçe/İngilizce açıklamaları Tablo 1'de verilmiştir.

Tablo 1: Kısaltmaların Türkçe/İngilizce açıklamaları

Kısaltma	İngilizce		Türkçe
IoT	Internet of Things	:	Nesnelerin İnterneti
GPS	Global Positioning System	:	Küresel Konumlama Sistemi
LIDAR	Laser Imaging Detection and Ranging	:	Işın Algılama ve Mesafe Ölçme
NFC	Near Field Communication	:	Yakın Alan İletişim
RFID	Radio Frequency Identification	:	Radyo Frekansıyla Tanımlama
DoS	Denial of Service	:	Hizmet Engelleme
DDoS	Distributed Denial of Service	:	Dağıtılmış Hizmet Engelleme
AI	Artificial Intelligence	:	Yapay Zekâ
ML	Machine Learning	:	Makine öğrenimi
SCADA	Supervisory Control and Data Acquisition	:	Merkezi Denetim ve Veri Toplama Sistemi
ADS-B	Automatic Dependent Surveillance-Broadcast	:	Otomatik Bağımlı Gözetim Yayını
ZTA	Zero Trust Architecture	:	Sıfır Güven Mimarisi
MFA	Multi-Factor Authentication	:	Çok Faktörlü Kimlik Doğrulama
2FA	Two Factor Authentication	:	İki Faktörlü Kimlik Doğrulama
PKI	Public Key Infrastructure	:	Açık Anahtar Altyapısı
IDS	Intrusion Detection Systems	:	Saldırı Tespit Sistemi
NIST	National Institute of Standards and Technology	:	Ulusal Standartlar ve Teknoloji Enstitüsü
CISA	Cybersecurity and Infrastructure Security Agency	:	Siber Güvenlik ve Altyapı Güvenlik Ajansı
Firewall		:	Güvenlik Duvarı
Ransomware		:	Fidye Yazılımı
Phishing		:	Oltalama

Bu bağlamda siber güvenliğin ulaşım sektörü özelindeki rolünü anlamak için yapılan çalışmanın ikinci bölümünde ulaşım sektöründe kullanılan IoT sistemleri,

üçüncü bölümünde ulaşım sektörüne yönelik yaygın kullanılan siber saldırılar, dördüncü bölümünde kara, hava, deniz gibi ulaşım sektöründe yaşanmış etkili siber saldırıları örnekleri detaylandırılmıştır. Son olarak bu saldırıları önlemeye yönelik öneriler verilerek çalışma bitirilmiştir.

2. Ulaşım Sektöründe Nesnelerin İnterneti Sistemleri

IoT uygulamaları farklı sektörlerde hızla yayılmakta ve ulaşım sektörü de bu dönüşümün önemli bir parçası haline gelmektedir. Trafik yönetiminde, trafik ışığı sensörleri, trafik yoğunluğu izleme sensörleri, akıllı yol işaretleri, hız kameraları ve dijital yol bilgilendirme ekranları kullanılarak, yolculukların daha verimli ve güvenli bir şekilde yönetilmesi sağlanmaktadır.

Araç takibinde GPS takip cihazları, telematik sistemler ve araç performans izleme sensörleri sayesinde araçların konumları ve durumu anlık olarak izlenebilmekte ve yönetilebilmektedir.

Akıllı park sistemlerinde, park yeri sensörleri ve park yeri bilgilendirme ekranları ile park yeri bulma süreci hızlandırılmakta ve trafik yoğunluğu azaltılmaktadır. Yol durumu izlemekte ise yol yüzeyi sensörleri, buzlanma tespit sensörleri, çevresel (hava durumu) izleme cihazları ve yol bozulma sensörleri kullanılarak sürücülere daha güvenli yol koşulları sunulmaktadır. Ayrıca, sıcaklık ve nem sensörleri, özellikle hassas yük taşımacılığında, çevresel koşulları izlemek için yaygın olarak kullanılmaktadır. Otonom araçlarda ise ışın algılama ve mesafe ölçme sensörleri, radar sensörleri ve otomatik sürüş sensörleri kullanılarak, sürüş güvenliği sağlanmakta ve çevre analizleri yapılmaktadır.

Yakın alan iletişim ve radyo dalga frekansıyla tanıma teknolojileri, akıllı biletleme, lojistik depolama ve ürün takibi gibi alanlarda kullanılmaktadır. Güvenlik açısından ise kameralar, kişilerin güvenliğini sağlamak, ürünlerin durumunu izlemek, bebek izleme gibi uygulamalarda ve otonom sürüş sistemlerinde yaygın olarak kullanılmaktadır.

IoT cihazlarının gelişimi, sensörlerin rolü, kullanılan sensör türleri ve IoT uygulamalarındaki teknolojiler ele alınmıştır. Sensörlerin, ulaştırma farklı sektörlerdeki ihtiyaçları karşılamak için çok çeşitli alanlarda kullanıldığı gösterilmiştir (Zhang & Tan, 2021)

Ulaşım sektöründe IoT teknolojilerinin kullanımı, trafik yönetimi, akıllı ulaşım sistemleri, otonom araçlar, elektrikli araç şarj istasyonları ve lojistik operasyonları gibi birçok alanda devrim niteliğinde gelişmeler sağlamaktadır (Thomas & Tine, 2025).

IoT cihazları, Araç-araç (V2V) ve Araç-altyapı (V2I) iletişimi, akıllı trafik kontrol sistemleri, hava ve deniz taşımacılığında otomasyon gibi uygulamalarda kullanılarak yakıt verimliliği, zaman tasarrufu ve operasyonel maliyetlerin azalması gibi önemli avantajlar sunmaktadır (Zeddini et al., 2022).

Özellikle otonom araçlar ve bağlantılı araç teknolojileri, IoT destekli sensörler ve iletişim sistemleri ile donatılarak çevresel farkındalığı artırmakta ve sürüş güvenliğini iyileştirmektedir (Illiashenko et al., 2023).

Benzer şekilde, elektrikli araç şarj istasyonları, IoT ile entegre edildiğinde dinamik fiyatlandırma, akıllı enerji yönetimi ve kullanıcı deneyimi optimizasyonu gibi yenilikler sağlamaktadır (Khan et al., 2024).

Lojistik ve tedarik zinciri yönetiminde, IoT cihazları gerçek zamanlı konum takibi, filo yönetimi ve envanter optimizasyonu gibi operasyonel süreçleri iyileştirerek teslimat sürelerini kısaltmakta ve kaynak kullanımını daha verimli hale getirmektedir (Ntafloukas et al., 2023).

Ancak, IoT teknolojilerinin hızla yaygınlaşması, ulaşım altyapılarının güvenliğini tehdit eden yeni siber saldırı risklerini de beraberinde getirmektedir. Bağlantılı ulaşım sistemlerinin artan saldırı yüzeyi, hizmet reddi saldırıları, fidye yazılımı, kimlik avı, GPS sahtekarlığı, veri ihlalleri ve nesnelerin interneti botnet saldırıları gibi tehditlerin ortaya çıkmasına neden olmaktadır (Tandan et al., 2025).

Endüstriyel kontrol sistemleri (ICS) ve akıllı ulaşım altyapıları, kötü niyetli aktörler tarafından hedef alındığında trafik yönetiminde aksaklıklar, havaalanı operasyonlarının durması veya limanlardaki lojistik süreçlerin sekteye uğraması gibi ciddi güvenlik ve ekonomik sonuçlar doğurabilmektedir (Tonn et al., 2019)

Özellikle havacılık sektöründe, uçak sistemlerinin otomatik bağımlı gözetim yayın (ADS-B) manipülasyonu ve GPS sinyal bozma (jamming) saldırılarına karşı hassas olduğu bilinmektedir (Eleimat & Őszi, 2025)

Deniz taşımacılığında ise akıllı liman sistemlerine yönelik kimlik avı saldırıları ve fidye yazılımları, operasyonları aksatmakta ve tedarik zinciri güvenliğini tehdit etmektedir (Al-Zahrani, 2022).

Bağlantılı araçlar akıllı trafik sistemleri ve lojistik süreçler gibi IoT destekli çözümler, ulaşım sektöründe büyük fırsatlar sunmaktadır. Bu fırsatlar sistemleri daha verimli hale gelirken, aynı zamanda yeni saldırı yöntemlerine karşı zafiyetlere de yol açmaktadır.

3. Ulaşım Sektörüne Yönelik Siber Saldırılar

IoT teknolojilerinin yaygınlaşmasıyla birlikte, ulaşım altyapıları daha önce hiç olmadığı kadar dijitalleşmiştir. Bu dijitalleşme, ulaşım sektörünü daha verimli hale getirmiş olsa da beraberinde önemli güvenlik risklerini de getirmiştir.

Aşağıda ulaşım sektörüne yönelik çeşitli siber saldırı türleri ve bu saldırıların potansiyel etkileri açıklanmıştır.

3.1. Hizmet Reddi ve Dağıtılmış Hizmet Reddi Saldırıları

Hizmet reddi (DoS) ve dağıtılmış hizmet reddi (DDoS) saldırıları, bir sisteme aşırı trafik göndererek veya sistemin kaynaklarını zorlayarak hizmetin kesilmesine neden olur. Özellikle DDoS saldırıları, çok sayıda farklı kaynaktan gelen trafikle gerçekleştirilir ve genellikle daha güçlüdür, bu da ulaşım sistemlerini daha uzun süre işlevsiz bırakabilir.

Havacılık ve akıllı ulaşım altyapılarında DDoS saldırılarının büyük kesintilere neden olduğu ve özellikle limanlar, havalimanları ve tren istasyonlarının bu saldırılara açık olduğu vurgulanmıştır (Thomas & Tine, 2025).

DDoS saldırılarının akıllı trafik yönetim sistemlerine ve otonom araçların kontrol mekanizmalarına nasıl zarar verebileceği ele alınmıştır. Akıllı trafik yönetim sistemleri üzerindeki zararlar ve otonom araçların kontrol mekanizmalarına etkileri üzerine çalışılmıştır. Bir akıllı kavşakta araç başına ortalama gecikme süresi %65 oranında arttığı, ortalama seyahat süresinin %39 arttığı ve trafik akışındaki verimliliğin %20 azaldığı gösterilmiştir (Zeddini et al., 2022).

3.2. Zararlı Yazılımlar ve Fidye Yazılımları

Zararlı yazılımlar ulaşım sistemlerine entegre edilen IoT cihazlarına bulaşarak sistemleri işlevsiz hale getirebilir. Diğer bir yaygın tehdit ise fidye yazılımlarıdır. Bu yazılımlar kullanıcı verilerini şifreleyerek ya da sistemleri kilitleyerek fidye talep eder, bu da sistemlerin normale dönmesini engelleyebilir.

Ulaşım sektörüne yönelik fidye yazılımı saldırıları giderek artmaktadır ve özellikle rezervasyon sistemleri, biletleme altyapıları ve lojistik yönetim sistemleri bu saldırılardan etkilenmektedir (Tandan et al., 2025).

Fidye yazılımı saldırılarının ulaşım tedarik zincirleri ve sigorta sistemleri üzerindeki finansal etkileri analiz edilmiştir. Özellikle denizcilik, havacılık, demiryolu ve kara taşımacılığı gibi alanlarda fidye yazılımı nedeniyle oluşabilecek kesintilerin etkisi değerlendirilmiştir. Kritik düğüm noktalarında yaşanan kesintilerin domino etkisiyle tüm sistemleri nasıl etkileyebileceği görülmüştür (Tonn et al., 2019).

3.3. Sosyal Mühendislik ve Oltalama Saldırıları

Sosyal mühendislik saldırıları, insan hatalarını ve zayıflıkları kullanarak bilgi çalmayı amaçlayan saldırılardır. Bununla birlikte oltalama saldırıları, sahte e-postalar veya web siteleri aracılığıyla kişisel bilgileri toplamakta ve ardından saldırıya geçilmektedir.

Havayolu şirketleri ve ulaşım sektöründeki çalışanlara yönelik sosyal mühendislik saldırıları incelenmiş ve bu saldırıların operasyonel güvenliği nasıl tehdit ettiği tartışılmıştır. Güvenlik-temelli emniyet analiz yöntemlerinin gerekliliği vurgulanmıştır. Ulaşım sistemlerinde güvenlik artık sadece yazılımla değil, yapay zekânın da entegre edildiği karmaşık bir süreç olarak ele alınmıştır (Illiashenko et al., 2023).

Havayolu sektöründe çalışan hesaplarının ele geçirilmesiyle yolcu bilgilerinin çalınmasına yönelik saldırılar ele alınmıştır. Yolcu bilgilerinin çalınmasına yönelik siber saldırılar, havayolu çalışanlarının kimlik bilgileri ve oturum bilgilerinin hedef alındığı saldırılar, rezervasyon sistemlerine yapılan izinsiz erişimler, sosyal mühendislik ile yapılan kimlik avı saldırıları anlatılmış ve örnekleri sunulmuştur (Eleimat & Őszi, 2025)

3.4. Otonom Araçlara Yönelik Saldırılar

Otonom araçlar, sürücüsüz hareket eden araçlar olup, IoT tabanlı sistemlere dayanır. Bu araçlar özelinde yapılan saldırılar, saldırganların araçların navigasyon ve kontrol sistemlerini hedef alarak otonom araçları devre dışı bırakmalarına veya kontrol etmelerine olanak tanımaktadır.

GPS sahteciliği saldırılarının otonom araçlar ve uçak sistemleri üzerindeki etkileri analiz edilmiştir. Uçak içi sistemler ve entegre haberleşme altyapılarının saldırıya açık olduğu, dolayısıyla GPS gibi konum belirleme sistemlerinin de bu tehditten etkilenebileceği vurgulanmıştır (Al-Zahrani, 2022).

Havacılık sektöründe otomatik bağımlı gözetim yayın (ADS-B) manipülasyonunun uçuş güvenliği için büyük bir risk oluşturduğu belirtilmiştir (Khan et al., 2024).

3.5. Fiziksel Cihaz Manipülasyonu

Saldırganlar IoT cihazlarının fiziksel olarak manipülasyonu yoluyla ulaşım sistemlerini hedef alabilir. Bu tür saldırılar sensörlerin değiştirilmesi veya cihazlara zarar verilmesi şeklinde gerçekleşebilir, bu da sistemlerin düzgün çalışmamasına neden olmaktadır.

Trafik ışıkları, otonom araçlar ve akıllı ulaşım altyapılarının IoT saldırılarına karşı savunmasız olduğu vurgulanmıştır (Ntafloukas et al., 2023).

Sanayi kontrol sistemlerine, merkezi denetim ve veri toplama sistemi (SCADA) ve liman vinç sistemlerine yapılan saldırıların, lojistik operasyonlarını aksattığı belirtilmiştir (Al-badawi, 2024).

3.6. Veri Sızdırma ve İhlali

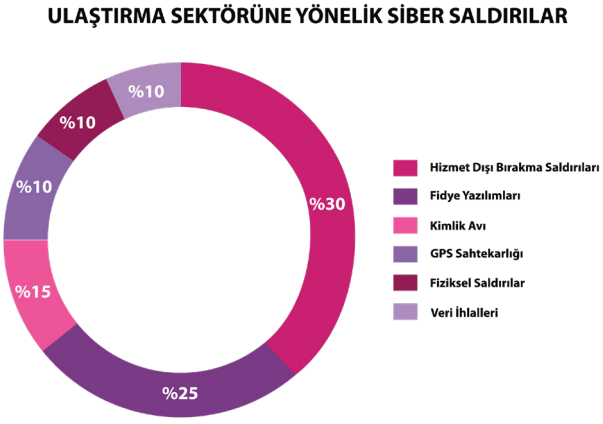
Siber saldırganlar, ulaşım sektörüyle ilgili hassas verileri çalarak veya kötüye kullanarak veri ihlali gerçekleştirebilir. Bu saldırılar genellikle kullanıcı bilgileri, güzergâh verileri, ticari bilgiler ve lojistik planlamalar gibi kritik verileri hedef almaktadır.

Yukarıda bahsedilen saldırı türlerinden etkilenen sistemler ise aşağıda listelenmiştir:

- Akıllı biletleme ve ödeme sistemleri
- Akıllı araçlar ve bağlı araç sistemleri
- Elektrikli araç şarj istasyonları

- GPS ve araç takip sistemleri
- Online ödeme ve lojistik yönetim sistemleri
- Otonom araçlar
- Otopark yönetim sistemleri
- Trafik yönetim sistemleri
- Yolcu bilgileri

Şekil 2.'de bu çalışma kapsamında ele alınan makalelerden elde edilen verilere göre ulaşım sektörüne yönelik saldırıların dağılım grafiği oluşturularak sunulmuştur (Thomas & Tine, 2025), (Tandan et al., 2025), (Illiashenko et al., 2023), (Al-Zahrani, 2022), (Ntafloukas et al., 2023), (Eleimat & Őszi, 2025).



Şekil 2: Ulaşım Sistemlerine Yönelik Siber Saldırı Dağılımı

4. Ulaşım Sektörüne Yönelik Siber Saldırı Örnekleri

Ulaşım sektörü artan dijitalleşme ile birlikte siber saldırılara karşı daha savunmasız hale gelmiştir. Havacılıktan deniz taşımacılığına, demiryollarından kara taşımacılığına kadar birçok alanda, kritik altyapıları hedef alan siber saldırılar, operasyonları aksatmakta ve büyük maddi kayıplara yol açmaktadır. Aşağıda, farklı ulaşım sektörlerine yönelik gerçekleşmiş önemli siber saldırılar ve bunların etkileri detaylandırılmıştır.

4.1. Havacılık Sektörüne Yönelik Siber Saldırılar

Havacılık sektörü, yüksek güvenlik standartlarına sahip olmasına rağmen siber saldırılardan kaçınamamaktadır. Özellikle hava yolu şirketleri, havalimanları ve uçak üreticileri, veri ihlalleri ve fidye yazılımı saldırılarının hedefi olmaktadır.

Boeing'in yedek parça bölümüne yapılan fidye yazılımı saldırısı ve Swissport'un maruz kaldığı siber saldırı, havalimanı operasyonlarını sekteye uğratmıştır. Benzer şekilde, British Airways ödeme sistemlerine yönelik veri ihlali, yüz binlerce yolcunun finansal bilgilerini tehlikeye atmıştır.

Tablo 2'de, havacılık sektörüne yönelik gerçekleşmiş büyük ölçekli siber saldırılar, bu saldırıların hedefleri ve sektöre olan etkileri üzerinde durulmuştur.

Tablo 2: Havacılık sektörüne yönelik yapılan siber saldırılar

Saldırı Adı	Yıl	Saldırı Türü	Hedef	Etkileri	Kaynak
Boeing	2023	Fidye Yazılımı	Boeing'in yedek parça bölümü	50 GB veri çalındı, fidye talep edildi	(Ishii, 2025)
Swissport	2022	Fidye Yazılımı	İsviçre merkezli havaalanı hizmet sağlayıcısı	Havalimanı operasyonları aksadı	(Pochmara & Świetlicka, 2024)
British Airways	2018	Veri İhlali	British Hava Yolu ödeme sistemleri	500.000 yolcunun finansal bilgileri çalındı	(Noah et al., 2024)
Delta Air Lines	2004	Zararlı Yazılım	Delta Hava Yolları bilgi sistemleri	Bilgisayar sistemleri devre dışı kaldı, uçuşlar iptal edildi	(Okero, 2024)

4.2. Denizcilik ve Limanlara Yönelik Siber Saldırılar

Deniz taşımacılığı küresel ticaretin bel kemiği niteliğinde olup siber saldırıların önemli hedeflerinden biridir. Belçika ve Hollanda'daki liman sistemlerine yönelik hizmet reddi saldırısı, lojistik sektöründe büyük aksamalara yol açmıştır. 2017 yılında Maersk'e yönelik NotPetya saldırısı, şirketin tüm IT altyapısını felç ederek yüz milyonlarca dolarlık zarara sebep olmuştur.

Denizcilik sektörüne yönelik büyük ölçekli siber saldırılar, yalnızca operasyonel süreçleri aksatmakla kalmayıp, küresel lojistik zincirlerinde de ciddi aksamalara yol açmaktadır. Denizcilik sektöründe yaşanan önemli siber saldırılar ve bunların sektöre etkileri Tablo 3'te aktarılmıştır.

Tablo 3: Denizcilik sektörüne yönelik yapılan siber saldırılar

Saldırı Adı	Yıl	Saldırı Türü	Hedef	Etkileri	Kaynak
Belçika ve Hollanda Limanları	2022	Hizmet Reddi	Avrupa'daki limanlardaki IT sistemleri	Lojistik sektöründe büyük aksamalara neden oldu	(Fenton, 2024)
Maersk NotPetya	2017	Fidye Yazılımı	Danimarka merkezli lojistik devi Maersk	Şirketin tüm IT sistemleri çöktü, 300 milyon dolar zarar oluştu	(Junction & Arbor, 2000)

4.3. Demiryolu ve Akıllı Ulaşım Sistemlerine Yönelik Siber Saldırılar

Demiryolları ve akıllı ulaşım sistemleri, siber tehditlere karşı kritik bir risk taşımaktadır. Hannover'de gerçekleştirilen siber saldırı simülasyonu, demiryolu sistemlerinin altı hafta içinde milyonlarca saldırıya maruz kaldığını ortaya koymuştur. Özellikle IoT tabanlı sinyalizasyon sistemleri ve akıllı trafik yönetim mekanizmaları hedef alındığında, bu saldırılar yalnızca anlık aksamalara değil, uzun vadede altyapının güvenliği ve yolcu güvenliğini de tehdit eden sonuçlara yol açabilmektedir. Akıllı ulaşım sistemlerine yönelik siber saldırılar, şehir içi ve şehirlerarası ulaşım ağlarında büyük aksamalara ve zincirleme güvenlik risklerine neden olabilmektedir.

Tablo 4'te, demiryolu ve akıllı ulaşım sistemlerine yönelik gerçekleşmiş önemli siber saldırılar ve bunların etkileri sunulmuştur.

Tablo 4: Demiryolu ve akıllı ulaşım sistemlerine yönelik siber saldırılar

Saldırı Adı	Yıl	Saldırı Türü	Hedef	Etkileri	Kaynak
Almanya Demiryolu Ağına Yönelik Siber Saldırı	2022	Hizmet Reddi ve Yetkisiz Erişim	Hannover demiryolu ağları	6 haftada 2.745.000 saldırı tespit edildi	(Antonio et al., 2025)
İspanya	2020	Fidye yazılımı	Altyapı yöneticisi firma	Kişisel ve ticari veri ifşası	(Korpimäki, 2023)

4.4. Kara Taşımacılığı ve Elektrikli Araçlara Yönelik Siber Saldırılar

Kara taşımacılığı ve elektrikli araç altyapıları da siber saldırganlar tarafından hedef alınmaktadır. Brokenwire saldırısı, elektrikli araç şarj istasyonlarını devre dışı bırakarak kullanıcıları mağdur etmiştir. 2021'de Colonial Pipeline'a yönelik fidye yazılımı saldırısı, ABD'nin doğu yakasında yakıt krizine yol açarak, siber saldırıların ekonomik etkilerinin ne denli büyük olabileceğini göstermiştir.

Kara taşımacılığı ve elektrikli araç altyapılarına yönelik en önemli siber saldırılar Tablo 5'te özetlenmiştir.

Tablo 5: Kara taşımacılığı ve elektrikli araç altyapılarına yönelik siber saldırılar

Saldırı Adı	Yıl	Saldırı Türü	Hedef	Etkileri	Kaynak
Brokenwire Saldırısı	2022	Kablosuz Saldırı	Elektrikli araç şarj istasyonları	Şarj işlemleri kesintiye uğratıldı	(Gupta et al., 2024)
Colonial Pipeline Fidye Yazılımı Saldırısı	2021	Fidye Yazılımı	ABD'deki petrol ve gaz boru hattı Colonial Pipeline	ABD'nin doğu yakasında yakıt krizi yaşandı	(Gawazah, 2024)

4.5. Microsoft Açıklarından Yararlanılarak Yapılan Siber Saldırılar

Microsoft'un yazılım açıkları, birçok sektörde olduğu gibi ulaşım sektöründe de siber tehditlerin kapısını aralamıştır. Microsoft Office yazılımlarındaki güvenlik açıkları, saldırganların zararlı belgeler aracılığıyla sistemlere sızmasını sağlamış ve saldırı oranlarını dört kat artırmıştır. Microsoft Bing'in back-end sunucusuna yönelik veri ihlali ise kullanıcı bilgilerinin açığa çıkmasına neden olmuştur.

Microsoft'un yazılım açıkları, ulaşım sektörü için ciddi bir güvenlik tehdidi oluşturmaktadır. Aşağıdaki tabloda bu açıkların nasıl kullanıldığına dair önemli örnekler verilmiştir.

Tablo 6: Microsoft yazılım açıklarından kaynaklanan siber saldırılar

Saldırı Adı	Yıl	Saldırı Türü	Hedef	Etkileri	Kaynak
Microsoft Office Açıklarına Yönelik Saldırılar	2018	Zararlı Yazılım	Microsoft Office yazılımlarındaki güvenlik açıkları	Zararlı Office belgeleri kullanılarak siber saldırılar 4 kat arttı	(Shahid & Safyan, 2025)

Genel olarak bakıldığında ulaşım sektöründe gerçekleşen siber saldırılar büyük ekonomik ve operasyonel kayıplara yol açmaktadır. Havacılık, denizcilik, demiryolu ve kara taşımacılığı gibi kritik alanlarda güvenliği artırmak ve saldırılara karşı önlem almak giderek daha önemli hale gelmiştir.

5. Ulaşım Sektöründe Siber Güvenlik Önlemleri

Bu çalışma kapsamında ulaşım sektöründe IoT sistemlerine yönelik makaleler ve Ulusal Standartlar ve Teknoloji Enstitüsü Siber Güvenlik Çerçevesi (NIST Cybersecurity Framework) raporları incelenerek ulaşım sektörüne yönelik siber saldırı ve tehditlere yönelik alınması gereken siber güvenlik önlemleri maddeler halinde sunulmuştur.

5.1. IoT Cihazları için Güvenlik Önlemleri ve Öneriler

IoT cihazları, trafik yönetimi, otonom araçlar, elektrikli araç şarj istasyonları, akıllı ulaşım altyapıları ve lojistik sistemleri gibi birçok alanda kritik görevler üstlenmektedir. Ancak bu cihazların güvenli olmaması hem sistemin bütünlüğünü hem de yolcu güvenliğini tehdit edebilir. Bu nedenle IoT cihazlarının güvenliğini sağlamak için aşağıdaki önlemler alınmalıdır:

5.1.1. Şifreleme ve Veri Koruma

IoT cihazlarından gelen verilerin kötü niyetli kişilerin eline geçmesini önlemek için uçtan uca veri şifreleme (end-to-end encryption) uygulanmalıdır. Hassas veriler, AES (Advanced Encryption Standard) veya RSA (Rivest-Shamir-Adleman) gibi güçlü şifreleme algoritmaları ile korunmalıdır. IoT cihazlarında blockchain tabanlı veri güvenliği sistemleri kullanılarak veri manipülasyonunun önüne geçilmelidir.

5.1.2. Kimlik Doğrulama ve Erişim Kontrolü

IoT cihazlarına yetkisiz erişimi önlemek için çok faktörlü kimlik doğrulama (MFA) kullanılmalıdır. Cihazlar arası güvenli iletişimi sağlamak için açık anahtar altyapısı (PKI) tabanlı dijital sertifikalar uygulanmalıdır. IoT cihazlarının sadece

yetkili ağlar üzerinden erişilebilir olması için erişim kontrol listeleri (ACL) ve ağ segmentasyonu sağlanmalıdır.

5.1.3. Yazılım Güncellemeleri ve Güvenlik Yamaları

Cihaz üreticileri yazılımlarındaki güvenlik açıklarını kapatmak için düzenli güncellemeler ve güvenlik yamaları (patch management) yayınlamalıdır. IoT cihazlarında otomatik güncelleme mekanizmaları kullanılarak, kullanıcıların manuel olarak güvenlik yamalarını yükleme zorunluluğu ortadan kaldırılmalıdır. Açık kaynak kodlu yazılım kullanılıyorsa, kod denetimi ve güvenlik testleri düzenli olarak gerçekleştirilmelidir.

5.1.4. Ağ Güvenliği ve Saldırı Tespit Sistemleri

IoT cihazlarının bağlı olduğu ağlar, güçlü güvenlik duvarları ve saldırı tespit sistemleri ile korunmalıdır. Olası anormallikleri tespit edebilmek için makine öğrenmesi tabanlı tehdit algılama sistemleri kullanılmalıdır. Sıfır güven mimarisi uygulanarak her bağlantının kimliği sürekli doğrulanmalı ve yetkisiz erişim engellenmelidir.

5.2. Kamu ve Özel Sektör İşbirliği ile Siber Güvenlik Politikaları

Ulaşım sektörü, hem kamu kurumları hem de özel şirketler tarafından işletilen sistemleri içerdiğinden, siber güvenlik politikalarının oluşturulmasında bu iki tarafın iş birliği büyük önem taşımaktadır. Güçlü bir ulaşım siber güvenlik stratejisi oluşturabilmek için aşağıdaki politikaların uygulanması önerilmektedir:

5.2.1. Yasal Düzenlemeler ve Standartlar

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ve ISO/IEC 27001 gibi uluslararası siber güvenlik standartlarına uyumluluk zorunlu hale getirilmelidir. Avrupa Birliği'nin NIS2 Direktifi ve ABD'de CISA (Cybersecurity and Infrastructure Security Agency) düzenlemeleri, ulaşım altyapısının korunmasına yönelik önemli rehberler sunmaktadır. Otonom araçlar ve IoT tabanlı ulaşım sistemleri için özel olarak tasarlanmış siber güvenlik çerçeveleri geliştirilmelidir.

5.2.2. Kamu-Özel Sektör İş Birliği Mekanizmaları

Hükümetler, özel ulaşım şirketleri ve siber güvenlik uzmanları arasında bilgi paylaşımı sağlanmalıdır. Siber tehdit istihbaratı paylaşım ağları kurularak, potansiyel saldırılar hakkında erken uyarı sistemleri oluşturulmalıdır. Ulaşım sektöründe siber güvenlik bilincini artırmak için kamu-özel sektör ortak eğitim programları düzenlenmelidir.

5.2.3. Acil Durum MÜdahale Planları ve Siber Sigorta

Ulaşım sektöründe siber olay müdahale ekipleri (CSIRT - Computer Security Incident Response Team) oluşturulmalıdır. Sigorta şirketleri, ulaşım altyapılarına

özel siber güvenlik poliçeleri geliştirerek fidye yazılımı saldırıları gibi tehditlere karşı finansal güvence sağlamalıdır.

5.3. Gelecekteki Tehditlere Karşı Alınması Gereken Önlemler

Ulaşım sektörü teknolojik gelişmelere paralel olarak yeni ve daha karmaşık siber saldırılara maruz kalmaktadır. Bu nedenle gelecekte ortaya çıkabilecek tehditlere karşı proaktif güvenlik önlemleri alınmalıdır:

5.3.1. Yapay Zekâ Destekli Tehdit Algılama ve Yanıt Sistemleri

Makine öğrenmesi ve yapay zekâ destekli tehdit tespit sistemleri, anormal ağ aktivitelerini tespit ederek erken uyarı sağlamalıdır. Davranışsal analiz sistemleri, anormal kullanıcı hareketlerini belirleyerek sahte girişleri ve veri sızıntılarını önleyebilir.

5.3.2. Kuantum Kriptografi ile Güvenli Haberleşme

Kuantum bilgisayarların klasik şifreleme yöntemlerini kırma potansiyeli göz önünde bulundurularak, post-kuantum kriptografi algoritmaları geliştirilmelidir. Kuantum anahtar dağıtımı (QKD) teknolojisi ile uçtan uca güvenli iletişim sağlanmalıdır.

5.3.3. Blok Zinciri Tabanlı Kimlik Doğrulama Sistemleri

Blok zincir teknolojisi kullanılarak nesnelerin interneti cihazları için merkezi olmayan kimlik doğrulama mekanizmaları oluşturulmalıdır. Akıllı ulaşım sistemlerinde veri manipülasyonlarını önlemek için akıllı kontratlar kullanılmalıdır.

5.3.4. Siber Tatbikatlar ve Senaryo Tabanlı Testler

Siber güvenlik tatbikatları düzenlenerek, ulaşım altyapısının saldırılara ne kadar dayanıklı olduğu test edilmelidir. Kritik altyapılara yönelik "Red Team" saldırı simülasyonları gerçekleştirilerek zafiyetler belirlenmelidir.

Sonuç

Yukarıda incelenen çalışmalar ve yapılan analizler neticesinde, ulaşım sektöründeki nesnelerin interneti (IoT) cihazlarının güvenliğinin sağlanmasına ilişkin öneriler aşağıda belirtilmiştir:

IoT Cihazlarına Yönelik Güvenlik Protokolleri: Ulaşım altyapısında kullanılan IoT cihazlarının güvenliği, genel siber güvenlik stratejilerinin temelini oluşturur. Her cihazın benzersiz kimlik doğrulama sistemleri ve şifreleme protokollerine sahip olması gerekir. Bu cihazlar arasındaki iletişimde, endüstri standardı güvenlik protokolleri (örneğin, TLS/SSL şifrelemesi) kullanılmalıdır.

Gerçek Zamanlı İzleme ve Anomali Tespiti: Ulaşım sistemlerinde, trafik yönetimi, otopark yönetimi, akıllı ulaşım araçları ve şarj istasyonları gibi kritik sistemlerin sürekli olarak izlenmesi gerekir. Anomali tespit sistemleri, normal dışı davranışları anında tespit edebilecek şekilde yapılandırılmalıdır. Bu, herhangi bir siber saldırı girişiminin erken safhada tespit edilmesini sağlar.

Ağ Ayrıştırma ve Mikrosegmentasyon: IoT cihazları ve diğer ulaşım altyapı sistemleri, siber saldırganların sistemler arasında hareket etmesini engellemek için ağ seviyesinde ayrıştırılmalıdır. Mikrosegmentasyon, her cihazı ve altyapı bileşenini kendi güvenlik duvarlarıyla izole eder ve sadece gerekli olan sistemler arasında iletişim sağlar.

Yapay Zekâ Destekli Saldırı Tespit Sistemleri: Ulaşım sektöründe siber saldırıların tespitini hızlandırmak için yapay zeka tabanlı sistemler kullanılabilir. Bu sistemler, geçmiş saldırı verilerinden öğrenerek potansiyel tehditleri daha doğru bir şekilde tespit edebilir. Ayrıca, makine öğrenmesi algoritmaları ile sahte trafik veya kötü amaçlı veri akışları tanımlanabilir.

Dijital Kimlik ve Erişim Yönetimi: Ulaşım sektöründeki kritik sistemlere erişimi yöneten dijital kimlik ve erişim yönetimi çözümleri, yalnızca yetkilendirilmiş kişilerin sisteme erişmesini sağlar. Çift faktörlü kimlik doğrulama (2FA) ve biyometrik doğrulama yöntemleri, sistem güvenliğini artıran etkili önlemlerden biridir.

Fiziksel Güvenlik ve Erişim Kontrolü: Özellikle şarj istasyonları, trafik yönetim sistemleri ve otonom araçlar gibi kritik altyapı noktalarında, fiziksel güvenlik önlemleri de büyük önem taşır. Cihazların ve sunucuların bulunduğu alanlara sadece yetkili personelin girmesi sağlanmalı, düzenli olarak güvenlik denetimleri yapılmalıdır.

Yedekleme ve Felaketten Kurtarma Planları: Ulaşım sistemleri için düzenli veri yedekleme ve felaketten kurtarma planları oluşturulmalıdır. Siber saldırılar sonucunda sistemlerin çökmesi veya veri kaybı yaşanması durumunda, sistemlerin hızlı bir şekilde eski haline getirilmesi için önceden belirlenmiş bir kurtarma prosedürü uygulanmalıdır.

Eğitim ve Farkındalık Çalışmaları: Tüm ulaşım sektörü çalışanlarına, siber güvenlik tehditlerine karşı farkındalık kazandırmak için düzenli eğitimler verilmeli ve bu konuda bilinçlendirme çalışmaları yapılmalıdır. İnsan faktörü, siber saldırıların en zayıf halkalarından biri olduğu için, personel güvenliği ön planda tutulmalıdır.

Regülasyon ve Standartlara Uyum: Ulaşım sektörü, küresel ve yerel siber güvenlik düzenlemeleri ve standartlarına uyum sağlamalıdır. Bu, hem yasal açıdan zorunlu olabilir hem de siber güvenlik risklerini minimize etmek için önemli bir adımdır. Avrupa Birliği'nin GDPR gibi veri güvenliği düzenlemeleri, sektördeki tüm oyuncular tarafından dikkate alınmalıdır.

Siber Güvensizlik ve Yeni Nesil Güvenlik Stratejileri: Bununla birlikte, tüm bu güvenlik önlemleri uygulanmış olsa da siber güvensizlik, ulaşım sektörü için hala ciddi bir tehdit oluşturabilmektedir. Siber güvensizlik, yalnızca teknik altyapıdaki açıklar ve zayıflıklardan değil, aynı zamanda organizasyonel eksikliklerden,

insan hatalarından ve sistematik yetersizliklerden kaynaklanmaktadır. Ulaşım sektöründeki IoT cihazlarının güvenliği, siber güvensizlikle mücadele etmek için yalnızca teknolojik çözümlerle değil, aynı zamanda organizasyonel, operasyonel ve insan faktörüne yönelik stratejilerle de ele alınmalıdır.

Sonuç olarak ulaşım sektöründe siber güvenlik risklerini minimize etmek ve siber güvensizlik ile etkin bir mücadele, sadece teknik altyapının güçlendirilmesi değil, aynı zamanda organizasyonel düzeyde de geniş kapsamlı bir güvenlik stratejisinin benimsenmesi ile mümkündür. Bu önlemler, ulaşım altyapılarının dijitalleşme sürecinde karşılaşılan siber tehditlere karşı daha dayanıklı hale gelmesini sağlayacaktır.

Kaynakça

Al-badawi, H. (2024). *Cyber Security Challenges in the Transportation Industry – A Comprehensive Analysis and Recommendations.* 11(2), 16–41. https://doi.org/10.12792/JMTI.11.2.16

Al-Zahrani, A. (2022). Assessing and Proposing Countermeasures for Cyber-Security Attacks. *International Journal of Advanced Computer Science and Applications,* 13(1), 885–895. https://doi.org/10.14569/IJACSA.2022.01301102

Antonio, J., Franco, D. P., & Pires, F. (2025). *Cyber Attacks against Critical Infrastructures Analysis of Methods , SCADA Exploitation and Real Cases.* 1–12.

Eleimat, M., & Őszi, A. (2025). *Cybersecurity in Aviation: Exploring the Significance, Applications, and Challenges of Cybersecurity in the Aviation Sector*. https://doi.org/10.3311/PPtr.37153

Fenton, A. J. (2024). Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore. *Journal of Marine Science and Engineering,* 12(3). https://doi.org/10.3390/jmse12030510

Gawazah, L. (2024). To Pay or Not to Pay- The US Colonial Pipeline Ransomware Attack. *Researchgate, August*. https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack

Gupta, K., Panigrahi, B. K., Joshi, A., & Paul, K. (2024). Demonstration of denial of charging attack on electric vehicle charging infrastructure and its consequences. *International Journal of Critical Infrastructure Protection*, 46(February), 100693. https://doi.org/10.1016/j.ijcip.2024.100693

Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., & Di Giandomenico, F. (2023). Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. *Entropy,* 25(8), 1–35. https://doi.org/10.3390/e25081123

Ishii, D. (2025). *Comparative Analysis of Major Cybersecurity Incidents : Major Cybersecurity Incidents in 2018. February,* 0–7. https://doi.org/10.13140/RG.2.2.18254.78407

Junction, W. R., & Arbor, A. (2000). *Developing a Culture of. 21*(1), 270–276.

Khan, I. U., Ouaissa, M., Ouaissa, M., Houda, Z. A. El, & Ijaz, M. F. (2024). Cyber Security for Next-Generation Computing Technologies. In *Cyber Security for Next-Generation Computing Technologies.* https://doi.org/10.1201/9781003404361

Korpimäki, S. (2023). *Cybersecurity and Risk Management in Implementing Future Railway Mobile Communications System.*

Macit, A. (2024). *Ulaştırma Modlarının Geleceği : Yapay Zekânın Akıllı Ulaşım Sistemlerine Entegrasyonu The Future of Transportation Modes : Integration of Artificial Intelligence into Intelligent Transportation Systems.* 0–2.

Neutze J., N. J. P. (2013). Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cybre Security Norms. *Georgetown Journal of International Affairs,* May 2025, 3–15.

Noah, A., Moon, L., & John, A. (2024). *The Consequences of Non-Compliance with Data Protection Regulations on Business Analytics Authors. December.*

Ntafloukas, K., Pasquale, L., Martinez-Pastor, B., & McCrum, D. P. (2023). A Vulnerability Assessment Approach for Transportation Networks Subjected to Cyber–Physical Attacks. *Future Internet,* 15(3). https://doi.org/10.3390/fi15030100

Okero, E. K. (2024). *Qualitative Study on Cyber Security Attacks Affecting the Civil Aviation Industry.*

Önder, H., & Akdemir, F. (2020). Digital Dimension of Urban Transportation: Transportation 4.0. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi,* 3(2), 202–215.

Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of Industrial Systems—A 2023 Report. Electronics (Switzerland), 13(7). https://doi.org/10.3390/electronics13071191

Shahid, M. A., & Safyan, M. (2025). *MALWARE ANALYSIS AND DETECTION FOR MICROSOFT TECHNOLOGIES.* 1(1), 57–69.

Tandan, B., Vajpayee, P., & Hossain, G. (2025). Explaining Cyber Risks in Transportaion 5.0: A Data Driven Approach. *2025 IEEE 4th International Conference on AI in Cybersecurity, ICAIC 2025, February,* 1–8. https://doi.org/10.1109/ICAIC63015.2025.10848812

Thomas, O., & Tine, J. (2025). *Cybersecurity in Transportation Systems : Policies and Technology Directions.*

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, 79(March), 103–114. https://doi.org/10.1016/j.tranpol.2019.04.019

Zeddini, B., Maachaoui, M., & Inedjaren, Y. (2022). Security Threats in Intelligent Transportation Systems and Their Risk Levels. *Risks,* 10(5), 1–18. https://doi.org/10.3390/risks10050091

Zhang, D., & Tan, P. (2021). Internet of Things and intelligent transportation system. *Journal of Physics,* 2066(1). https://doi.org/10.1088/1742-6596/2066/1/012066