

Havacılık Yönetiminde Yapay Zekâ Dijital Kimlik

Zuhal Erdem¹

Özet

Havacılık endüstrisi, yapay zekânın hızlı gelişimiyle yönlendirilen benzeri görülmemiş bir dönüşüm sürecindedir. Yapay zekânın havacılıkta kullanımı; güvenliği, verimliliği ve yolcu deneyimini iyileştirerek sektörde köklü bir değişim yaratmaktadır. Bu bölümde, havayolu işletmelerinde yapay zekâ temelli sistemlerin dijital kimlik süreçlerine entegrasyonu incelenmiştir. Özellikle IATA tarafından geliştirilen “Proje 777” ve “Proje 321” tasarımları örnek olay olarak ele alınmış; bu projelerin teknik altyapıları, güvenlik, emniyet ve karar destek sistemlerine katkıları ayrıntılı biçimde değerlendirilmiştir. Ayrıca, projelerin etik ve şeffaflık boyutları da tartışılmıştır. Söz konusu tasarımlar, güvenlik açıklarını en aza indirerek, tekrarlayan süreçleri ortadan kaldırmakta ve insana bağımlılığı azaltarak havayolu operasyonlarını hızlandırmaktadır. Dijital kimlik çözümlerinin benimsenmesi hem yasal düzenlemelere hem de güvenlik gerekliliklerine uyumu güçlendirmekte; aynı zamanda yolcu deneyimini yeniden şekillendirmektedir. Bu teknolojik dönüşüm, hava yolculuğunun geleceğini tanımlayarak onu daha güvenli, daha akıllı ve daha kullanıcı odaklı bir hale getirmektedir.

1.Giriş

Tüm sektörlerde önemli görevler üstlenen yapay zekânın havacılık sektöründe de önemi günden güne artmaktadır. Havacılık endüstrisi yenilikçi yaklaşımları yakından takip ederek hız kazanmaktadır. Havacılık endüstrisi tarih boyunca, uçuşları daha emniyetli, verimli ve erişilebilir kılmak amacıyla sürekli yeniliklere odaklanmış ve birçok teknolojik devrim geçirmiştir (Jiang vd., 2023). Günümüzde havayolu işletmeleri, yapay zekâdan yararlanarak yolcular için daha fazla değer yaratmayı hedeflemektedir.

1 Dr., Turkish Airlines Cabin Crew Directorate /Instructor, e-mail: zsakici@gmail.com, ORCID: 0000-0002-1694-7800

Yapay zekâ artık insan yaşamının vazgeçilmez bir bileşeni haline gelmiştir. Doğal zekânın taklit edilmesi anlamına gelen bu teknoloji, insana özgü bilişsel süreçlerin yazılımlar aracılığıyla makinelere aktarılmasını ifade etmektedir (Farrow, 2019).

Günümüzde havacılık sektörü ile yapay zekâ birbirinden ayrı düşünülemez. Uçakların kuşlarla aynı sonucu (uçma) elde etmesi ancak farklı mekanizmalarla gerçekleştirmesi gibi, yapay zekâ da insan düşünme biçimlerini farklı yöntemlerle simüle etmektedir. Bu sayede makineler, insan zekâsının birçok yönünü taklit ederek verileri analiz edebilmekte, örüntüleri tanımlayabilmekte, karar alabilmekte ve problemleri çözebilmektedir.

Havacılıkta yapay zekâ teknolojileri çok çeşitli alanlarda uygulanmaktadır. Havayolu işletmeleri, tahmini bakım planlaması ve müşteri hizmetlerinde yapay zekâ odaklı otomasyon sistemlerini benimserken; biyometrik tanımlama sistemleriyle yolcuların güvenlik kontrolleri ve uçağa geçiş prosedürlerini kolaylaştırmaktadır. Gelişmiş biyometrik sistemler sayesinde güvenlik tarama süreleri azalmış, tehdit tespitindeki doğruluk oranı ise artmıştır. Çevik havayolu işletmeleri ayrıca mobil uygulamalar ve ödeme sistemleri gibi dijital platformlarını modernize ederek daha kusursuz bir yolculuk deneyimi sunmaktadır.

Akıllı havalimanları, güvenliği artırmak amacıyla gelişmiş algılama ve kontrol sistemlerinden yararlanırken; bulut bilişim ve büyük veri analitiği, uçuş planlamasının, yakıt tüketiminin ve müşteri etkileşimlerinin kişiselleştirilmesinin optimizasyonunda kullanılmaktadır. Yapay zekâ, rota optimizasyonundan hava trafiği tahminine ve risk öngörüsüne kadar hava sahası yönetiminde de verimliliği ve güvenliği artırmaktadır (International Civil Aviation Organization, 2025).

Ayrıca yapay zekâ destekli rota optimizasyonu, çevresel sürdürülebilirlik açısından yakıt tasarrufu sağlamaktadır. Üretken yapay zekâ, doğal dil arayüzleri aracılığıyla havayolu işletmelerine erişilebilir çözümler sunarak; ekip planlaması, tedarik zinciri yönetimi ve kriz müdahalesinde öngörü gücünü artırmakta, böylece güvenilirlik ve maliyet verimliliğini yükseltmektedir.

Havacılık işletmeleri, yapay zekâ sayesinde yolcu ihtiyaçlarını ve çevresel unsurları gerçek zamanlı olarak değerlendirebilmekte; ürün ve hizmetlerini farklılaştırarak kişiselleştirebilmektedir. Bu durum, işletmelere önemli bir rekabet avantajı kazandırmaktadır (Meydan, 2023).

Yapay zekânın görevleri otomatikleştirme ve verileri gerçek zamanlı analiz etme yeteneği, havacılık profesyonellerinin sistemlerle etkileşim biçimini dönüştürmekte; bu da verimlilik, güvenlik ve karar alma süreçlerinde yeni

fırsatlar yaratmaktadır. Yapay zekâ, veri analitiği, makine öğrenimi, derin öğrenme ve nesnelerin interneti gibi yöntemlerle bütünleşik bir ekosistem oluşturmaktadır.

Veri analitiği ve yapay zekânın entegrasyonu, gerçek zamanlı tehdit tespitini ve hızlı müdahaleyi mümkün kılmaktadır. Havayolu işletmeleri, veri analitiği sayesinde gerçek talebe uygun ikram hazırlıkları yaparak gıda israfını ve aşırı üretimi azaltabilmektedir (Singh, 2025).

Makine öğrenmesi, verilerden bağımsız olarak öğrenme ve tahmin üretme becerisiyle, yolcu deneyimini iyileştiren algoritmalar geliştirmektedir. Bu algoritmalar, yolcuların yaşadığı deneyimlere ilişkin verileri (örneğin uçuş gecikmeleri, bagaj teslim süresi, check-in süresi, uçak içi hizmet kalitesi vb.) analiz ederek memnuniyet skorlarını tahmin edebilmektedir. Böylece belirli yolcu profillerine göre gelecekteki memnuniyet düzeyi öngörülmekte, potansiyel sorunlara proaktif çözümler geliştirilebilmektedir (Alanazi vd.,2024).

Havayolu müşterileriyle güçlü ve işbirlikçi ilişkiler kurmak, sadakati artırmak ve ekonomik değeri yükseltmek için entegre yolcu verisi gerekliliği giderek artmaktadır (Alshurideh vd., 2019).

Derin öğrenme, makine öğrenmesinin bir alt kümesi olup yapay sinir ağları üzerinden karmaşık veri kümelerinden çıkarım yapmayı hedefler. Bu algoritmalar, milyonlarca parametreyi işleyerek yolcu memnuniyeti analizlerinde yüksek doğruluk sağlamaktadır. Yolcuların geçmiş tercihleri, geri bildirimleri ve sosyal medya etkileşimleri incelenerek kişiselleştirilmiş hizmetler önerilmektedir. Bu sayede, sürekli veri analizi yoluyla misafir deneyimi daha etkili biçimde optimize edilmektedir (Bullchand, 2020).

Nesnelerin İnterneti (IoT), insan müdahalesi olmaksızın veri iletimi gerçekleştiren akıllı cihazlardan oluşan bir sistemdir (Singh vd., 2020). IoT teknolojisi sayesinde hava kargo gönderileri gerçek zamanlı olarak takip edilebilmekte; GPS uçakların izlenmesine, RFID sistemleri ise yüklerin sürekli gözetimine olanak tanımaktadır. Bu durum hırsızlık ve kaybolma risklerini en aza indirerek operasyonel güvenilirliği artırmaktadır (Şahan, 2025).

Sektörün temel bileşenlerinden olan havayolu işletmeleri, bilgi sistemlerini operasyonel faaliyetlerde ve paydaş ilişkilerinde yoğun biçimde kullanmaktadır. Yapay zekânın havayolu operasyonlarına entegrasyonu sayesinde zaman ve iş gücü tasarrufu sağlanmakta, maliyetler düşürülmekte ve rekabet avantajı elde edilmektedir. Ayrıca büyük veri analitiğiyle güvenlik

süreçleri optimize edilmekte, operasyonel dönüşüm stratejik bir boyut kazanmaktadır.

Yapay zekânın veri odaklı doğası, işletmelerin süreçlerini veri temelli bir bakış açısıyla yeniden yapılandırmasını zorunlu kılmaktadır. Bu doğrultuda, dijital kimlik kullanımı güvenlik, verimlilik ve kişiselleştirme açısından kritik bir unsur haline gelmiştir. Dijital kimlik için yenilikçi çözümler geliştirmek, havacılık sektöründe sürdürülebilir büyümenin ve güvenliğin temel koşulu olarak değerlendirilmektedir.

2.Dijital Kimlik

Bilgi güvenliği, dijital çağın en temel gereksinimlerinden biridir. Dijitalleşmenin hızlanmasıyla birlikte veriye erişim ve kullanılabilirlik artmış; buna paralel olarak güvenlik ve mahremiyet riskleri de çeşitlenmiştir. Kişisel veri, günümüzde “internetin yeni yakıtı” olarak tanımlanmakta ve her geçen gün daha stratejik bir değer kazanmaktadır.

Veriye erişimin kolaylaşması, özellikle havayolu işletmeleri açısından ciddi güvenlik ve gizlilik sorunlarını beraberinde getirmiştir. Yolculara ait verilerin manipüle edilememesi, kopyalanamaması ve üçüncü kişiler tarafından izinsiz erişilememesi kritik bir gerekliliktir. Bu doğrultuda dijital kimlik çözümleri, veri sızıntısı riskini en aza indirirken, şifrelenmiş veri üzerinden gerçekleştirilen kimlik doğrulama mekanizmaları sayesinde kullanıcıların güvenli bir biçimde hizmet almasını mümkün kılmaktadır (European Commission, 2023).

Dijital kimlik, sanal ortamda bir bireyi veya kurumu tanımlayan ve yazılımlar tarafından doğrulanabilen kimlik bilgilerinden oluşan bir yapıdır (Windley, 2005). Ancak dijital ortamdaki belgelerin çoğu, fiziksel belgelerin dijitalleştirilmiş kopyalarıdır ve bu belgelerin kolaylıkla taklit edilebilmesi, doğrulama süreçlerinde güven sorunları yaratmaktadır. Bu nedenle hem bireylerin hem de kurumların belgelerini dijital ortamda güvenli biçimde sunabilecekleri, imza ve kişisel bilgilerin dijital olarak doğrulanabileceği bir altyapıya ihtiyaç duyulmaktadır. Böyle bir yapı, belgelerin güvenilir biçimde sunulmasını ve doğrulanmasını sağlayarak olası güvenlik açıklarını büyük ölçüde ortadan kaldıracaktır (Doğan ve Karacan, 2022).

2.1 Dijital Kimlik Yönetim Modelleri

Dijital kimlik yönetimi, bir bireyin ya da kuruluşun kimliğinin güvenli, doğrulanabilir ve sürdürülebilir biçimde tanımlanmasını sağlayan sistematik bir yapıdır. Dijitalleşmenin hız kazanmasıyla, kimlik doğrulama süreçleri yalnızca teknik bir gereklilik olmaktan çıkıp stratejik bir güvenlik unsuru

haline gelmiştir. Bu kapsamda geliştirilen kimlik yönetim modelleri, veri gizliliği, erişim kontrolü ve kullanıcı deneyimi arasındaki dengeyi korumayı amaçlamaktadır.

Her model, kimlik doğrulama süreçlerinde farklı derecelerde merkeziyet, kullanıcı kontrolü ve veri paylaşım politikası sunmaktadır. Aşağıda bu modellerin temel özellikleri ve işleyiş prensipleri ele alınmaktadır.

2.1.1 Merkezi Kimlik Yönetimi (Centralized Identity Management)

Merkezi kimlik yönetimi, kullanıcıların kimlik bilgilerinin tek bir veri tabanında toplandığı ve erişim yetkilerinin merkezi bir sistem tarafından denetlendiği yapıdır. 1990'lı yılların ortalarından itibaren gelişen Active Directory ve LDAP (Lightweight Directory Access Protocol) teknolojileriyle yaygınlık kazanmıştır. Bu modelde kullanıcı kimlikleri tek bir veri kaynağında tutulur, erişim izinleri merkezi biçimde yönetilir ve sistem yöneticileri kullanıcı yetkilerini kapsamlı bir şekilde denetleyebilir. Kimlik doğrulama, merkezi servisler üzerinden gerçekleştirilir; bu da yönetimi kolaylaştırırken, yüksek düzeyde erişim kontrolü sağlar (Blockchain Türkiye Platformu [BCTR], 2025).

2.1.2 Federe Kimlik Yönetimi (Federated Identity Management)

Federe kimlik yönetimi, farklı kuruluşlar veya servis sağlayıcıları arasında kimlik bilgisinin paylaşılmasına olanak tanıyan bir yaklaşımdır. Bulut tabanlı hizmetlerin ve sistem entegrasyonlarının yaygınlaşmasıyla önem kazanmıştır.

Bu modelde kullanıcılar, tek bir kimlikle birden fazla sisteme erişebilir. Single Sign-On (SSO) teknolojisi ve SAML (Security Assertion Markup Language) protokolü, bu yapının temelini oluşturmaktadır. Tek oturum açma özelliği sayesinde kullanıcı bir kez giriş yaptıktan sonra, farklı sistemler arasında yeniden kimlik doğrulaması yapmadan geçiş yapabilir. Federe sistemler, OpenID Connect ve OAuth gibi protokollerle uyumlu çalışır. Ayrıca Avrupa Birliği ülkelerinde yürürlükte olan eIDAS (Electronic Identification and Trust Services for Electronic Transactions in the Internal Market) düzenlemesi, bir ülkede geçerli olan ulusal kimlik sistemlerinin diğer AB ülkelerinde de geçerli olmasını sağlamaktadır (European Union, 2014).

2.1.3 Kullanıcı Merkezli Kimlik Yönetimi (User Centric Identity Management)

Kullanıcı merkezli kimlik yönetimi, kimlik sahibine kendi verileri üzerinde tam kontrol hakkı tanıyan bir yaklaşımdır. 2010'lu yılların sonlarından itibaren

yaygınlaşan bu modelde kullanıcı, kimlik bilgilerinin nasıl kullanılacağına ve kimlerle paylaşılacağına kendisi karar verir.

Bu yaklaşımda kimlik doğrulama süreçleri özelleştirilebilir; kullanıcı yalnızca gerekli bilgileri, dilediği taraflarla paylaşır. Bu yönüyle model, veri sahipliği, mahremiyet ve kişisel kontrol ilkelerini güçlendirir (BCTR, 2025).

2.1.4 Kullanıcı Egemen Kimlik Yönetimi (Self Sovereign Identity Management)

Bu modelde dijital kimlik verileri, kimlik sahibinin kendi cihazında bulunan dijital kimlik cüzdanlarında saklanır. Kimlik sağlayıcı kuruluşlardan alınan veriler, üçüncü taraf altyapılarına bağımlı olmaksızın kullanıcı tarafından yönetilir ve paylaşılır.

2015 yılından itibaren öne çıkan bu yaklaşım, merkezi yapıları ortadan kaldırarak veri egemenliğini tamamen kullanıcıya devretmiştir. Bu sayede, kimlik bilgilerinin kontrolü, saklanması ve iptali tamamen kullanıcı tarafından yürütülmektedir (Ünal & Uluyol, 2020). Yeni nesil dijital iş modellerinin, güvenli, hızlı ve kullanıcı merkezli kimlik doğrulama sistemleri üzerine inşa edilmesi beklenmektedir.

Bu kitap bölümünde, IATA tarafından geliştirilen Proje 777 ve Proje 321 tasarımları çerçevesinde dijital kimlik çözümleri incelenmektedir. Her iki proje de, IATA ve sektör paydaşlarının birlikte yürüttüğü bir kavram kanıtı (Proof of Concept – PoC) niteliğindedir. Ayrıca, söz konusu çözümlerin güvenlik, emniyet ve karar destek sistemlerine katkıları ile etik ve şeffaflık konularındaki yansımaları da ayrıntılı biçimde ele alınmaktadır.

3. Proje 777 (7 Yeni İş Akışıyla 7 İş Gününden 7 Saniyelik Kayıt Sürecine)

3.1 Projenin Amacı ve Kapsamı

Havacılık sektörü, yapay zekânın verimlilik, müşteri deneyimi ve operasyonel mükemmelliğin temel unsurlarından biri haline geldiği kritik bir dönüşüm döneminden geçmektedir. Dijital kimlik, yalnızca teknik bir yenilik değil; aynı zamanda veri güvenliğinin, kimlik doğrulamanın ve dijital hakların yeniden tanımlandığı küresel ölçekte bir paradigma değişimini temsil etmektedir.

Proje 777, dijital kimlik yönetimini seyahat operasyonlarına entegre ederek, havayolları ve acente ortakları için güvenli, verimli ve kullanıcı dostu bir sistem oluşturmayı amaçlamaktadır. Bu kapsamda, kısa ve orta vadede

hem müşterilerin hem de ekosistem aktörlerinin dijital kimlik sahibi olmaları hedeflenmektedir.

Hâlihazırda acentelerin kimlik doğrulama yöntemleri mevcut olsa da acenteye bağlı kullanıcıların kimliklerinin yönetimi, dolandırıcılığın önlenmesi ve yönetim süreçlerinin sadeleştirilmesi açısından kapsamlı bir dönüşüme ihtiyaç duyulmaktadır.

Seyahat endüstrisi, dünya genelindeki acente operasyonlarının bütünlüğünü ve güvenilirliğini korumak amacıyla güvenli, verimli ve kusursuz bir dijital kimlik yönetimi sisteminin uygulanmasından büyük fayda sağlamayı amaçlamaktadır. Bu sistemin temelinde, dijital cüzdanlar ve dijital çalışan kimlikleri bulunmaktadır. Bu araçlar, operasyonların hızlandırılmasını, veri güvenliğinin artırılmasını ve insan hatasının en aza indirilmesini mümkün kılmaktadır.

Dijital kimlik altyapısı sayesinde seyahat acenteleri ve havayolu işletmeleri yalnızca güvenliği artırmakla kalmayacak, aynı zamanda operasyonel süreçleri de kolaylaştıracak güçlü ve esnek bir dijital kimlik çerçevesi kazanacaktır. Böylelikle sektör, daha güvenli, bütünlük ve verimli bir geleceğe doğru ilerleyecektir.

Bu çözümler, kullanıcı erişimlerinin etkin biçimde yönetilmesini ve devre dışı bırakılmasını kolaylaştırarak dolandırıcılık riskini azaltmakta, genel operasyonel etkinliği ise artırmaktadır. Standartlaştırılmış kimlik doğrulama ve dolandırıcılığı önleme yaklaşımları, hassas verilerin korunmasını sağlarken aynı zamanda dayanıklı ve bağlantılı bir seyahat ekosisteminin kurulmasına katkı sunmaktadır.

Acentelere, çalışanlarına ait dijital kimlik bilgilerini verme, yönetme ve gerektiğinde iptal etme yeteneği kazandırılmaktadır. Bu doğrultuda, kimlik bilgilerinin güvenli biçimde saklanabilmesi için dijital kimlik cüzdanlarının oluşturulması gerekmektedir.

Sektörde, farklı havayolu işletmelerine ait portallarda güvenliği artıracak, çoklu oturum açma gereksinimini ortadan kaldıracak birleşik kimlik doğrulama çerçevesi oluşturma ihtiyacından hareketle Proje 777 geliştirilmiştir.

Bu proje kapsamında, ön koşul olarak acentelerin bir IATA kodu edinmeleri, bir dijital cüzdan seçmeleri ve kendi kriptografik tanımlayıcılarını IATA kodlarıyla birlikte sistem dizinine kaydetmeleri gerekmektedir.

Geliştirilen Kavram Kanıtı (Proof of Concept - PoC) çalışması, dört farklı havayolu işletmesinin B2B (Business to Business) portalıyla etkileşime giren

acente çalışanlarına odaklanmış ve yedi adımlı bir iş akışını doğrulamıştır. Bu portallardan üçü doğrudan havayolu işletmeleri tarafından yönetilmekte; kimlik doğrulama süreçleri ise birden fazla teknoloji sağlayıcısının sunduğu doğrulanabilir kimlik bilgisi (Verifiable Credentials) hizmetleriyle entegre edilmektedir.

Bu PoC çalışması, kimlik belgesi oluşturma (seyahat acenteleri tarafından), dijital cüzdan kullanımı (mobil ve web tabanlı), ve çoklu doğrulama mekanizmalarını bir araya getirerek uçtan uca birlikte çalışabilirlik (interoperability) sağlamaktadır.

Projenin yedi adımlı iş akışı şu şekilde tanımlanmıştır:

1. Temsilci kimlik bilgilerini verecek kuruluş tarafından, acenteye dijital çalışan kimliği atanır.
2. Dijital cüzdan özelliği aracılığıyla oluşturulan başvuru formu doldurularak kuruluş kaydı tamamlanır (tüm havayolu işletmeleri bu özelliği kullanmayabilir).
3. Ortak kuruluş profiline bağlı acente dijital kimliğiyle yapılan başvurular otomatik onaylanır; ancak bu süreç, her havayolu işletmesinin onay politikalarına bağlı olarak farklılık gösterebilir.
4. Havayolu portalına ilk girişte acente bilgileri otomatik olarak sisteme iletilir, yeterlilik doğrulaması yapılır ve kullanıcı profili kendiliğinden oluşturulur.
5. Mobil kimlik doğrulaması, mobil uygulama üzerinden gerçekleştirilir.
6. Masaüstü kimlik doğrulaması, masaüstü uygulaması aracılığıyla yapılır.
7. Acentenin dijital kimliğini yalnızca temsilci kimlik bilgilerini veren yetkili kuruluş iptal edebilir (International Air Transport Association [IATA], 2025a).

3.2 İşleyiş ve Sistem Roller

Kavram kanıtı (Proof of Concept - PoC) kapsamında üç farklı seyahat acentesi çalışanına, mobil ve web tabanlı olmak üzere iki ayrı dijital cüzdan türü aracılığıyla dijital çalışan kimlikleri verilmiştir. Bu çalışanlar, dört farklı havayolu işletmesinin B2B portallarında kayıt ve giriş işlemlerini başarıyla gerçekleştirmiştir.

Sürecin son aşamasında, bir çalışanın kimliği acente tarafından iptal edildiğinde, ilgili kişinin tüm portallardaki erişim yetkileri otomatik olarak

kaldırılmıştır. Bu durum, kimlik doğrulama mekanizmasının merkezi otoritelerden bağımsız, güvenli ve birlikte çalışabilir bir yapıya kavuştuğunu göstermektedir. Bu yapının temel bileşenleri aşağıda özetlenmiştir:

Sistem Roller

- **Issuer (Veren Kurum):** Seyahat acentesi, çalışanlarına doğrulanabilir kimlik belgeleri (Verifiable Credentials) tahsis eden kurumdur. Bu belgeler, acente tarafından oluşturulmakta ve güvenilir kimlik sağlayıcı aracılığıyla doğrulanabilir şekilde yapılandırılmaktadır.
- **Holder (Sahip):** Seyahat acentesi çalışanı, kendisine verilen doğrulanabilir kimlik belgesini dijital cüzdanında güvenli biçimde saklar. Gerek duyulduğunda, bu kimliği yetkili doğrulayıcılarla paylaşabilir veya erişim iznini iptal edebilir.
- **Verifier (Doğrulayıcı):** Havayolu işletmeleri, acentelerin kimliklerini ve yetkilerini doğrulayan otorite konumundadır. Doğrulama süreci, merkezi bir veritabanına ihtiyaç duymadan, kriptografik imzalar ve güven zinciri prensipleri üzerinden yürütülmektedir.
- **Verifiable Data Registry (VDR):** Her acentenin web alanına bağlı bir dijital kayıt sistemidir. Bu sistem, kimliklerin oluşturulma, geçerlilik ve iptal kayıtlarını tutar. VDR yapısı, verilerin bütünlüğünü garanti altına alırken kimlik güncellemelerini eş zamanlı olarak tüm doğrulayıcılara yansıtır.
- **Trust Registry (Güven Kayıt Sistemi):** Yetkili kimlik veren kurumların listesini, geçerli kimlik türü şemalarını ve doğrulama kurallarını içeren merkezi bir referans dizinidir. Güven Kayıt Sistemi, sistemdeki tüm kimlik doğrulama işlemlerinin yetkili ve güvenilir kurumlar tarafından yürütülmesini garanti eder (IATA, 2025a).

Bu yapı, dağıtık kimlik altyapısının, havacılık sektöründe pratik olarak uygulanabilir olduğunu göstermektedir. Böylece, hem kimlik yönetiminde güvenlik düzeyi artırılmakta hem de operasyonel iş akışlarında zaman tasarrufu sağlanmaktadır.

3.3 Teknik Uyum ve Standartlar

Kavram Kanıtı (Proof of Concept – PoC), farklı teknoloji sağlayıcılarının çözümlerinin birlikte çalışabilirliğini garanti eden bir Interoperability Profile (Birlikte Çalışabilirlik Profili) üzerine inşa edilmiştir. Bu profil, kullanılacak kimlik formatlarını, kriptografik yöntemleri ve güvenlik mekanizmalarını

tanımlayarak sistemin teknik uyumunu ve bütünlüğünü sağlamaktadır. Bu kapsamda, süreçte yer alan temel standartlar şu şekilde yapılandırılmıştır:

- **Kimlik Verilmesi (OpenID for Verifiable Credential Issuance- OID4VCI):** Cüzdan ile kimlik veren kurum arasındaki belge oluşturma ve iletim sürecini tanımlar.
- **Kimlik Sunumu (OpenID for Verifiable Presentations- OID4VP):** Dijital kimliklerin doğrulayıcıya nasıl ve hangi güvenlik katmanlarıyla sunulacağını belirler.
- **Seçmeli Veri Paylaşımı (Selective Disclosure- SD-JWT VC):** Kimlik sahibinin yalnızca gerekli bilgileri paylaşmasına olanak tanıyarak veri minimizasyonu ve mahremiyet ilkelerini güçlendirir.
- **Kimlik İptali (OAuth 2.0 Credential Status List):** Kimlik belgelerinin geçerlilik durumlarını (aktif/iptal) yönetir ve sistemin güncel kalmasını sağlar.
- **Tanımlayıcı Metodu (Decentralized Identifier Method- did:web):** Kimlik belgelerinin doğrulanmasını web alanı üzerinden gerçekleştirerek merkezi otoritelerden bağımsız bir doğrulama mekanizması sunar.
- **Kriptografi Standartları (P-256 / secp256r1, ES256- JWT):** Dijital imza ve veri güvenliğini sağlayan endüstri standardı kriptografik yöntemleri temsil eder.

Bu standartların birlikte uygulanması sayesinde sistem, veri gizliliği, güvenilirlik ve şeffaflık ilkelerini koruyarak uluslararası düzeyde ölçeklenebilir bir dijital kimlik yönetimi çözümü sunmaktadır.

Dijital kimlik sürecinin bir parçası olarak seyahat acenteleri, çalışanlarına kimlik belgesi verebilmek için öncelikle Güven Kayıt Sistemi (Trust Registry)'ne kayıt olmalıdır. Bu sayede sistemdeki havayolu işletmeleri, kayıtlı acenteler tarafından verilen kimlik belgelerine otomatik olarak güven duyabilmektedir.

Her acente, kendi çalışanlarına ait doğrulanabilir kimlik belgelerini oluşturmakta ve bu belgeleri kendi DID (Decentralized Identifier) kimlikleriyle ilişkilendirmektedir. Acentenin DID kimliği, doğrudan kendi alan adıyla eşleştirilmekte; bu da kimliklerin bütünlüğünü, doğrulanabilirliğini ve izlenebilirliğini güvence altına almaktadır.

Verilen kimliklerin aktif veya iptal durumları, sistem tarafından sürekli olarak güncellenmektedir. Seyahat acentesi çalışanları için oluşturulan doğrulanabilir kimlik belgeleri; ad-soyad, kimlik numarası, iletişim bilgileri

(telefon ve e-posta), çalışan sicil numarası, unvan ve görev bilgilerini içermektedir. Süreç akışı aşağıdaki gibi ilerlemektedir.

- **Hazırlık:** Acentenin kriptografik anahtarları oluşturulmakta ve DID belgesi internet üzerinde erişilebilir hale getirilmektedir.
- **Güvenli Kayıt:** Acentenin DID ve IATA kodu, güvenilir yayıncılar listesine eklenmektedir.
- **Kimlik Verilmesi:** Doğrulanabilir kimlik belgesi acente çalışanın cihazına güvenli biçimde iletilmektedir.
- **Sunum Başlatma:** Çalışan, işletmeden işletmeye portalına giriş için QR kodu tarar; bu işlem, kimlik sunum sürecini başlatmaktadır.
- **Doğrulama:** Havayolu, kimliği kriptografik olarak doğrulamakta, belge geçerliliğini ve yayıncı güvenilirliğini kontrol etmektedir.
- **Revizyon ve Yetki Denetimi:** İlgili kimlik iptal edilmişse erişim reddedilmekte; aktifse sistem girişine izin verilmektedir (IATA, 2025a).

Proje 777, kimlik doğrulama süreçlerini “7 iş gününden 7 saniyeye” indirme vizyonuyla, dijital dönüşümün havacılık sektöründe kurumsal düzeyde uygulanabilirliğini kanıtlamaktadır. Dijital çalışan kimlikleri ve doğrulanabilir kimlik belgeleri, seyahat acenteleri ile havayolu işletmeleri arasındaki iş ilişkilerinde endüstri standardı haline gelerek; siber güvenlik risklerini azaltmayı, operasyonel süreçleri hızlandırmayı ve müşteri memnuniyetini artırmayı hedeflemektedir.

3.4 Proje 777’de Kullanılan Yapay Zekâ

Proje 777 kapsamında yapay zekâ teknolojileri, özellikle veri doğrulama, risk analizi ve davranış modelleme süreçlerinde temel bir rol oynamaktadır. Erişim taleplerinin doğruluğunu değerlendirmek amacıyla, geçmiş erişim kayıtlarını (acente bilgileri, cihaz türü, IP adresi, işlem tipi vb.) analiz eden denetimli makine öğrenmesi (Supervised Machine Learning) yöntemleri kullanılmıştır.

Bu süreçte Random Forest Classifier, Gradient Boosting Trees (XGBoost) ve Support Vector Machines (SVM) algoritmalarıyla eğitim yapılmıştır. Modeller, geçmiş erişim örüntülerini öğrenerek, acente kimliği ile sistem erişim davranışları arasındaki tutarsızlıkları tespit etmektedir. Örneğin, kısa süre içinde farklı ülkelerden yapılan girişleri anomali olarak algılayıp, olası siber saldırı veya dolandırıcılık girişimlerini önceden belirleyebilmektedir.

Anomali Tespiti (Anomaly Detection) aşamasında ise, sahte kimlik veya çoklu erişim girişimlerinin tespiti için denetimsiz öğrenme (Unsupervised

Learning) yöntemlerinden yararlanılmıştır. Isolation Forest ve Autoencoder tabanlı algoritmalar, erişim verilerinde istatistiksel sapmaları analiz ederek “olağandışı kullanıcı davranışlarını” tespit etmekte ve bu durumları sistem yöneticilerine raporlamaktadır. Böylece manuel denetim gereksinimi yaklaşık %70 oranında azalmıştır.

Ayrıca, acenteler tarafından gönderilen kayıt belgelerinin ve metin tabanlı başvuruların doğrulanması için doğal dil işleme (Natural Language Processing – NLP) destekli veri doğrulama mekanizmaları kullanılmıştır. Bu kapsamda Named Entity Recognition (NER) ve Optical Character Recognition (OCR) bileşenleri, Transformer tabanlı NLP modelleriyle entegre edilmiştir.

Bu modeller, başvuru belgelerindeki kimlik, unvan, adres, IATA kodu gibi bilgileri otomatik olarak tanımlayıp, veri tabanındaki referanslarla karşılaştırarak doğrulama işlemini gerçekleştirmektedir. Bu sayede hem doğruluk oranı artmış hem de manuel veri işleme süresi büyük ölçüde azalmıştır. Sonuç olarak, yapay zekâ tabanlı otomasyonun entegrasyonu sayesinde kimlik doğrulama ve kayıt onay süresi 7 iş gününden yalnızca 7 saniyeye indirilmiştir (IATA, 2025a).

3.5 Proje 777'nin Güvenlik ve Emniyet Sistemlerine Katkısı

Proje 777, havacılıkta işletmeden işletmeye (B2B) etkileşimlerde kullanılan kimlik sistemlerini dijitalleştirerek güvenliği güçlendirmeyi ve emniyet yönetimini standartlaştırmayı hedeflemiştir.

Proje kapsamında geliştirilen dijital çalışan kimliği ve doğrulanabilir kimlik belgeleri mekanizması, havayolları ile acenteler arasındaki erişim denetimini kriptografik olarak doğrulanabilir bir yapıya dönüştürmüştür. Yetkisiz erişimlerin önlenmesi konusunda bu sistem, her bir kullanıcının kimliğini kriptografik imzalarla doğrulamakta; böylece sahte hesap oluşturma veya üçüncü taraf erişimi olasılığını ortadan kaldırmaktadır. Bu özellik hem bilgi güvenliği hem de işlemsel bütünlük açısından kritik bir ilerleme sağlamaktadır.

Geleneksel parola tabanlı kimlik sistemlerinin en zayıf yönlerinden biri, kimlik hırsızlığı ve veri ihlalleri riskidir. Örneğin, 2018 yılında yaşanan British Airways veri ihlali sonucunda 500.000 yolcunun kişisel bilgileri ele geçirilmiştir. Bu tür olaylar, geleneksel sistemlerin kırılganlığını göstermektedir. Proje 777 ile kullanılan doğrulanabilir kimlik belgeleri sayesinde kimlik sahteciliği ve dolandırıcılık riskleri büyük ölçüde azaltılmış, kullanıcı kimlikleri güçlü bir kriptografik doğrulama zinciri içinde korunur hale gelmiştir (Noah vd., 2024).

Her kimliğin Güven Kayıt Sistemi (Trust Registry) üzerinde kayıtlı bir IATA kodu ve kriptografik kimlikle ilişkilendirilmiş olması, kimlik taklidi veya yetkisiz işlem gibi tehditleri minimize etmektedir. Ayrıca sistem, denetlenebilirlik ve izlenebilirlik açısından yüksek güvenlik seviyesi sunmaktadır. Tüm erişim hareketleri dijital olarak imzalandığı için, sistemde yapılan her işlem kayıt altına alınmakta; bu da olası bir siber saldırı ya da olay sonrası analizde kanıt temelli inceleme yapılabilmesini mümkün kılmaktadır (IATA, 2025a).

Projenin, kurumsal emniyet kültürüne katkısı da dikkat çekicidir. Otomatik kimlik doğrulama süreçleri, insan kaynaklı hataları azaltarak kurum içi emniyet farkındalığını ve güvenli davranış kültürünü güçlendirmektedir. Personel değişimleri veya görev devirlerinde yaşanabilecek erişim açıkları, sistem tarafından otomatik olarak kapatılmakta; bu da operasyonel süreçleri daha izlenebilir ve güvenilir hale getirmektedir (IATA, 2025b).

Böylece Proje 777, hem dolandırıcılık ve sahteciliği önleme hem de emniyet yönetimini dijital temelde güçlendirme yönünde sektörel bir standart oluşturmaktadır. Bu yaklaşım, ICAO Annex 19’da belirtilen Emniyet Yönetim Sistemi (Safety Management System – SMS) ilkeleriyle tam uyum içindedir ve emniyet kültürünün kurumsal düzeyde sürdürülebilirliğine doğrudan katkı sağlamaktadır (International Civil Aviation Organization [ICAO], 2016).

3.6 Proje 777’nin Karar Destek Sistemlerine Katkısı

Proje 777, havayolu işletmeleri ile acenteler arasındaki iş süreçlerinde dijital kimlik doğrulaması ve otomatik erişim yönetimi sağlayan bir işletmeden işletmeye (B2B) çözüm olarak tasarlanmıştır. Bu yapı, karar destek sistemleri açısından veri doğruluğunu, bütünlüğünü ve güvenilirliğini artırarak önemli bir değer üretmektedir.

Dijital çalışan kimlikleri sayesinde, sisteme giren her veri kriptografik olarak imzalanmış kimliklerle ilişkilendirilmekte ve böylece veri kaynağının doğrulanabilirliği sağlanmaktadır. Örneğin, herhangi bir bilet satış işleminin hangi acente personeli tarafından, hangi tarih ve IP adresiyle gerçekleştirildiği kesin biçimde kayıt altına alınmaktadır. Bu yaklaşım, karar destek sistemlerinde kullanılan verilerin güvenilirlik katsayısını artırmakta, aynı zamanda veri kirliliği ve yanlış analiz riski gibi sorunları ortadan kaldırmaktadır.

Süreç şeffaflığı ve izlenebilirlik açısından bakıldığında, Proje 777’nin Güven Kayıt Sistemi (Trust Registry) altyapısı, her işlem adımının kayıt altına alınmasını ve izlenebilirliğini sağlamaktadır. Bu veriler, karar destek

sistemlerinde denetim temelli analiz fonksiyonlarına entegre edilerek stratejik değerlendirmelere katkı sunmaktadır.

Örneğin, sistem yöneticileri veya IATA analistleri, hangi bölgelerde dolandırıcılık riskinin arttığını ya da hangi acentelerin olağandışı işlem yoğunluğuna sahip olduğunu gerçek zamanlı olarak görebilmektedir. Böylece hem operasyonel hem de stratejik düzeyde hızlı ve kanıta dayalı karar alma süreçleri mümkün hale gelmektedir.

Ayrıca dijital kimlik verileri, insan kaynakları, operasyonel yönetim ve erişim kontrol modülleri gibi karar destek alt sistemlerine doğrudan entegre edilebilmektedir. Bu sayede çalışan yetkilendirmesi, erişim iptali, bölgesel risk sınıflandırması gibi karar süreçleri otomatik ve dinamik bir yapıya kavuşmaktadır (IATA, 2025a).

Sonuç olarak Proje 777, dijital kimlik yönetimi ile karar destek sistemleri arasında güçlü bir köprü kurarak, yöneticilerin stratejik kararlara odaklanmasını, operasyonel kararların ise hızlı, güvenilir ve veri temelli biçimde alınmasını sağlamaktadır.

3.7 Proje 777'nin Etik ve Şeffaflık Sorunları

Proje 777, işletmeden işletmeye ekosisteminde dijital çalışan kimliklerini ve acente erişim yetkilerini doğrulayan bir sistemdir. Her ne kadar bu sistem dolandırıcılığı önlemeyi ve süreçleri hızlandırmayı hedeflese de beraberinde çeşitli etik ve mahremiyet temelli sorunlar doğurmaktadır.

Çalışan mahremiyeti açısından değerlendirildiğinde, dijital çalışan kimliklerinin her işlemle bireye özgü kriptografik bir kimlik ilişkilendirmesi, teorik olarak hesap verebilirliği artırsa da aşırı gözetim riskini de beraberinde getirmektedir. Her erişim, işlem ve sistem etkileşiminin kayıt altına alınması, çalışan davranışlarının sürekli izlenmesi anlamına gelebilmektedir. Ayrıca kurumsal veri saklama süresinin belirsizliği, işyeri mahremiyeti ve çalışan özgürlüğü ilkeleriyle çelişebilecek bir duruma yol açmaktadır (ECAT, 2024).

Makine öğrenmesi modelleri, özellikle anomali tespiti ve erişim kontrolü algoritmalarında geçmiş verilerle eğitildiğinden, örtük önyargılar içerebilir. Örneğin belirli coğrafi bölgelerdeki erişimler tarihsel olarak “şüpheli” olarak etiketlendiyse, model bu bölgelere sistematik biçimde ayrımcı sonuçlar üretebilir. Bu durum, adalet ve eşitlik ilkeleri açısından risk taşımakta; karar süreçlerinde tarafsızlık algısını zedeleyebilmektedir.

Ayrıca, proje kapsamında acenteler tarafından verilen dijital kimliklerin IATA kayıt sistemine eklenmesi gerekmektedir. Ancak bu verilerin saklama süresi, üçüncü taraflarla paylaşımı ve kullanıcı rızasının geri çekilmesi süreçleri

açık biçimde tanımlanmamıştır. Bu durum, GDPR Madde 7 uyarınca rıza geri çekme hakkı açısından uyumsuzluk riski oluşturmaktadır (European Union, 2018).

Bir diğer sorun, yapay zekâ tabanlı erişim kontrol kararlarının şeffaflığı ile ilgilidir. Erişim taleplerinin hangi kriterlere göre “şüpheli” olarak işaretlendiği veya reddedildiği kullanıcıya açıklanmamaktadır. Kullanıcı, neden erişimin askıya alındığını bilemediği için karar süreci “kara kutu (black box)” niteliği taşımakta; bu da sistemin hesap verebilirlik düzeyini zayıflatmaktadır (Çevik ve Akleyek, 2022).

Ayrıca sistem hataları veya yanlış sınıflandırmalarda sorumluluğun hangi aktöre ait olduğunun belirsizliği, etik sorumluluk zincirinde bir boşluk yaratmaktadır. Bu durum, dijital kimlik yönetimi altyapısının sadece teknik değil, aynı zamanda etik yönetim ilkeleriyle desteklenmesi gerektiğini göstermektedir.

4.Proje 321 Misafir Salonuna Erişim 3 Dakika’dan 1 Saniye’ye

4.1 Projenin Amacı ve Kapsamı

Proje 321, dijital kimlik, biyometri, veri paylaşımı ve gizlilik standartlarını bütüncül bir modelde birleştirerek, küresel havacılık endüstrisinin dijital dönüşüm stratejisine katkı sunmaktadır. Havacılık sektörü, yolcu kimliğinin doğrulanması, güvenlik ve müşteri deneyimi alanlarında dönüşümsel bir aşamadan geçmektedir. Projenin amacı, bir yolcunun tüm havalimanı süreçleri (rezervasyon, check-in, güvenlik ve biniş) boyunca tek bir dijital kimlik aracılığıyla doğrulanmasını sağlamaktır.

Geleneksel havalimanı süreçleri hâlâ pasaport, biniş kartı ve manuel kimlik doğrulama adımlarına dayandığından; yoğun hatlarda uzun bekleme süreleri, hatalı kimlik eşleştirmeleri ve artan operasyonel maliyetler ortaya çıkmaktadır. Proje 321, dijital kimlik ve biyometri teknolojilerinin entegrasyonu sayesinde bu süreçleri kâğıtsız, temassız ve gerçek zamanlı kimlik doğrulama temeline oturtmayı hedeflemektedir.

4.2. İşleyiş ve Sistem Roller

Proje 321’in kavram kanıtı çalışması (PoC), dijital kimlik, biyometrik doğrulama, güvenli veri paylaşımı ve çok paydaşlı sistem entegrasyonu unsurlarını bir araya getirmiştir. Proje, “Tek Kimlik- Tek Seyahat (One Identity - Seamless Travel)” vizyonuna dayanmaktadır. Hedef, yolcu deneyimini uçtan uca dijitalleştirerek hem operasyonel verimliliği artırmak hem de kişiselleştirilmiş, güvenli ve hızlı bir seyahat deneyimi sunmaktır.

Sistem Roller:

- DID (Decentralized Identifier): Her yolcuya özgü kriptografik kimliktir.
- Verifiable Credential (VC): Resmî kimlik verilerinin doğrulanabilir dijital formatıdır.
- Digital Wallet: Kimliklerin saklandığı güvenli dijital platformdur.
- Biometric Template: Yüz tanıma ve kimlik eşleştirme algoritmasıdır.
- Trust Registry: Kimlik doğrulama sağlayıcılarını doğrulayan güven altyapısıdır.

Kavram kanıtına Emirates, Qatar Airways ve Air France-KLM katılmış; teknoloji sağlayıcıları olarak Microsoft Azure Identity Platform ve SITA Smart Path görev almıştır. Deneme senaryosu Doha Hamad Uluslararası Havalimanı'nda gerçekleştirilmiştir. Bu sayede, dijital kimliği önceden oluşturulan yolcular, check-in ve biniş süreçlerinde fiziksel belge ibraz etmeden seyahat edebilmiştir (IATA, 2025a).

4.3 Teknik Uyum ve Standartlar

Proje, veri gizliliğini merkeze alan bir mimariyle geliştirilmiştir. Yolcunun kişisel bilgileri merkezi sunucular yerine cihaz üzerindeki dijital cüzdana saklanmaktadır. Hiçbir merkezi sistem, yolcunun kişisel verisini saklamamakta; tüm doğrulama işlemleri kriptografik kanıtlarla gerçekleştirilmektedir.

Sistem, uluslararası kimlik ve gizlilik standartlarıyla tam uyum içindedir:

- W3C Verifiable Credential: Kimlik verilerinin tanımlanması.
- ISO/IEC 19794-5: Biyometrik veri formatı standardı.
- OAuth 2.0/ OpenID: Yetkilendirilmiş veri paylaşımı.
- GDPR ve ICAO Annex 9: Gizlilik ve veri koruma ilkeleri

(European Union, 2018).

Bu standartların birlikte uygulanması, sistemin hem regülasyonlara uyumlu hem de küresel ölçekte birlikte çalışabilir olmasını sağlamaktadır.

Süreç Akışı:

1. Hazırlık: Yolcu mobil uygulama üzerinden dijital kimliğini oluşturur.
2. Güvenli Kayıt: Devlet veya güvenilir kurum kimliği doğrular ve VC olarak cüzdana ekler.

3. Kimlik Verilmesi: Biyometrik veriler (yüz, iris, parmak izi) kimliğe bağlanır.
4. Sunum Başlatma: Havalimanı kameraları yolcuyu tanır.
5. Doğrulama: Dijital kimlik çağrılır, kriptografik doğrulama yapılır.
6. Revizyon ve Yetki Denetimi: Kimlik doğrulandıktan sonra biniş kartı otomatik aktive edilir.

Merkezi olmayan mimari sayesinde, sistem tekil arıza noktalarını ortadan kaldırmakta ve siber saldırılara karşı dayanıklılık kazanmaktadır (Takçı, 2020). Proje 321, misafir salonuna erişim süresini 3 dakikadan 1 saniyeye indirerek güven, hız ve şeffaflığı aynı anda sağlamayı amaçlamaktadır.

4.4 Proje 321’de Kullanılan Yapay Zekâ

Proje 321, dijital kimlik ile biyometrik doğrulamayı birleştiren yolcu odaklı bir yapay zekâ sistemidir. Yapay zekâ burada özellikle görüntü işleme, yüz tanıma, öngörüselleştirme ve eşleştirme süreçlerinde kullanılmaktadır.

Derin öğrenme tabanlı Convolutional Neural Networks (CNN) modelleri-örneğin ResNet-50, MobileNetV3, FaceNet ve ArcFace- kullanılarak dijital kimlik ile biyometrik görüntü arasında %99,8 doğruluk oranına ulaşılmıştır. Canlılık tespiti katmanı sayesinde fotoğraf veya video yoluyla kimlik taklidi girişimleri engellenmiştir.

Ayrıca yoğunluk tahmini, güvenlik riski değerlendirmesi ve yolcu akış optimizasyonu için Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) ve Gradient Boosted Regression Trees gibi modellerle öngörüselleştirme yapılmaktadır. Bu modeller, geçmiş uçuş saatleri, kapı kullanımı ve doğrulama sürelerini analiz ederek gelecekteki yoğunlukları tahmin etmekte, yöneticilerin önleyici operasyonel kararlar almasını sağlamaktadır (Jiang vd, 2022).

Şüpheli kimlik veya çift kayıtlı tespiti için Hybrid AI yapısı (kural tabanlı + makine öğrenmesi) kullanılmıştır. Örneğin bir yolcunun dijital kimliği aynı anda iki farklı lokasyonda tarandığında, sistem bunu potansiyel güvenlik ihlali olarak işaretlemektedir. Bu yapı, ICAO Doc 9985 – Biometrics Implementation Guide standardıyla uyumludur (ICAO, 2013).

4.5 Project 321’in Güvenlik ve Emniyet Sistemlerine Katkısı

Proje 321, dijital kimlik ile biyometrik doğrulama (yüz/iris tanıma) teknolojilerini birleştirerek uçtan uca güvenli bir seyahat deneyimi sunmaktadır. Biyometrik veriler yolcunun dijital kimliğiyle eşleştirilerek çok

faktörlü bir doğrulama mekanizması oluşturulmuştur. Bu sistem, pasaport veya biniş kartlarının çalınması, sahte basımı ya da devri riskini ortadan kaldırmakta; kimlik doğrulamasını saniyeler içinde yüksek güvenilirlikle gerçekleştirmektedir.

Bu yaklaşım, Machine Readable Travel Documents (MRTD) ve EU Digital Identity Framework (eIDAS 2.0) standartlarıyla örtüşmektedir (ICAO, 2019). Ayrıca, Elmarady ve Rahouma'ya göre (2023) havacılıkta güvenlik ihlallerinin yaklaşık %45'inin insan hatalarından kaynaklandığı dikkate alındığında, Proje 321 manuel kontrollerdeki hataları azaltarak operasyonel emniyeti artırmaktadır. Temassız doğrulama, bulaşıcı hastalık risklerini de azaltarak pandemi sonrası dönemde havacılık güvenliğinde yeni bir paradigma yaratmıştır.

4.6 Proje 321'in Karar Destek Sistemlerine Katkısı

Proje 321, biyometrik doğrulama verilerini gerçek zamanlı olarak sistemlere aktararak karar destek süreçlerinde önemli bir işlev üstlenmektedir. Terminal içi yolcu konumu, yoğunluk ve işlem süreleri gibi bilgiler analiz edilerek kapı planlaması, güvenlik noktası optimizasyonu ve kalabalık yönetimi kararları desteklenmektedir (AI ve EUROCONTROL, 2020).

Ayrıca yapay zekâ tabanlı veri analitiği, geçmiş yolcu davranışlarını inceleyerek gelecekteki yoğunlukları ve potansiyel güvenlik risklerini öngörebilmektedir. Örneğin, belirli bölgelerde yinelenen kimlik hataları veya geç doğrulamalar, sistem tarafından risk temelli güvenlik önlemlerinin geliştirilmesi için kullanılmaktadır. Bu yapı, proaktif karar alma mekanizmaları oluşturulmasına olanak tanımaktadır.

4.7 Proje 321 Etik ve Şeffaflık Sorunları

Proje 321, biyometrik veriler (yüz, iris, parmak izi) ile dijital kimlikleri entegre eden bir sistemdir. Bu yapı güvenlik açısından güçlü olsa da etik ve mahremiyet bakımından karmaşık riskler barındırmaktadır. Biyometrik veriler değiştirilemez nitelikte olduğundan, bir veri sızıntısı durumunda bireyin geri döndürülemez mahremiyet kaybı söz konusu olmaktadır (Alshamaileh, 2023). Bazı pilot uygulamalarda yolcular dijital kimlik sistemlerini kullanmaya zorlanmış; alternatif manuel doğrulama yöntemleri sunulmamıştır. Bu durum, bilgilendirilmiş rıza ilkesinin ihhalidir. Yapay zekâ çağında kişisel veriler ile anonim veriler arasındaki sınırlar bulanıklaşmakta; görünürde “kişisel olmayan” veriler bile işlenerek birey tanımlanabilir hale gelebilmektedir. Ayrıca, insan denetiminden yoksun algoritmaların önyargı veya ayrımcılık içeren kararlar üretebildiği gözlemlenmiştir. Bu tür önyargılı

kararlar, sistematik ayrımcılık riskini artırmaktadır (Abudureyimu ve Oğurlu, 2021).

Veri paylaşımı açısından da şeffaflık eksiklikleri mevcuttur. Biyometrik verilerin hangi kurumlarla (havayolu işletmeleri, devlet otoriteleri, sınır güvenlik kurumları) ve ne süreyle paylaşıldığı belirsizdir. Sistemin bir kimliği yanlış reddetmesi durumunda, yolcu hangi algoritmanın kararı verdiğini veya nasıl itiraz edebileceğini bilmemektedir. Bu durum, algoritmik şeffaflık eksikliğinin açık bir örneğidir. Avrupa Komisyonu, bu tür sorunların önüne geçmek için Yapay Zekâ Düzenlemeleri (EU AI Act) ve etik denetim mekanizmaları geliştirmektedir (ECAT, 2024). Bu düzenlemeler, yapay zekâ sistemlerinde hesap verebilirliği ve denetlenebilirliği artırmayı hedeflemekte; Proje 321 gibi uygulamaların gelecekte etik yönden daha sağlam temellere oturmasını öngörmektedir.

5.Projelerin Kazanımları

Proje 777 ve Proje 321, havacılık sektöründe yapay zekâ destekli dijital kimlik yönetimi alanında güvenlik, operasyonel istikrar ve stratejik karar kalitesi bakımından sürdürülebilir bir dönüşümün önünü açmaktadır. Her iki proje de IATA'nın yapay zekâyı, insan kararlarını destekleyen ve geliştiren bir unsur olarak konumlandığını göstermektedir. Proje 777, acenteler açısından değerlendirildiğinde, havayolu rezervasyon platformlarına yalnızca doğrulanmış ve yetkilendirilmiş kullanıcıların erişebilmesini sağlayarak sahtecilik ve kimliğe bürünme riskini sınırlandırmaktadır. Acentelerin profillerini doğrudan sistem erişimleriyle ilişkilendirmesi, idari işlemleri azaltmakta ve kayıt sürecini hızlandırmaktadır. Tüm platformlarda ortak kullanılan birleşik kimlik doğrulama mekanizması, çoklu kullanıcı hesaplarının yönetimini kolaylaştırmakta; kimlik iptalleri merkezi olarak yönetildiği için yetkisiz erişimler engellenmektedir. Kullanıcıya mobil veya web tabanlı doğrulama seçenekleri sunulması, erişim sürecinde esneklik sağlamaktadır. Böylece acenteler açısından güvenlik ve verimlilik artarken, havayolu işletmeleri için operasyonel güvenilirlik güçlenmektedir.

Proje 321 ise yolcular açısından değerlendirildiğinde, dijital kimlik doğrulama süresini dakikalardan saniyelere indirerek zaman tasarrufu sağlamaktadır. Fiziksel kimlik veya belge gösterme zorunluluğunun ortadan kalkması, havalimanı geçişlerinde hız kazandırmakta ve yoğun hatlarda bekleme sürelerini azaltmaktadır. Çok dilli yapay zekâ çözümleri, farklı dillerdeki yolcularla iletişim engelini ortadan kaldırarak kişiselleştirilmiş bir seyahat deneyimi sunmaktadır. Otomatik dil tercihleri, kullanıcıya özgü öneriler ve yönlendirmelerle yolcu memnuniyeti artmakta; bu da

Net Tavsiye Skoru gibi memnuniyet göstergelerine olumlu yansımaktadır. Havayolu işletmeleri açısından bakıldığında, dijital kimlik doğrulamanın standart hale gelmesi dijital temas noktalarında daha yüksek oturma oranları sağlamakta, bu da gelir artışı ve müşteri bağlılığı potansiyeli yaratmaktadır. Kontuarlarda görev yapan personelin iş yükünün azalması operasyonel verimliliği yükseltirken, yapay zekânın hata payını azaltmasıyla hatalı kimlik eşleşmeleri büyük ölçüde azalmış ve dolandırıcılık riski düşmüştür.

Dijital kimliğin düzenli kullanımı yaygınlaştıkça, kimlik doğrulama yalnızca yasal işlemlerle sınırlı kalmayacak; misafir salonu erişimleri, sadakat programı üyelikleri ve diğer hizmet bağlantılarında da yaygın biçimde kullanılacaktır. Bu gelişmeler, yolcuların seyahat süreçlerini daha akıcı, hızlı ve güvenli hale getirmekte; aynı zamanda sektör genelinde veri bütünlüğü ve hizmet standardizasyonu sağlamaktadır (IATA, 2025a). Havalimanlarında güvenlik kontrol noktalarındaki yoğunluk azalmakta, yolcu akışı daha öngörülebilir hale gelmektedir. Uçak kapı planlamaları ve biniş zamanlamaları optimize edilerek operasyonel gecikmelerin önüne geçilmektedir.

Günümüz yolcuları, hız, esneklik ve temassız hizmet beklentilerinde giderek daha talepkâr hale gelmiştir. Yapay zekâ tabanlı sistemler, tekrarlayan görevleri azaltarak hem yolcular hem de acenteler için daha etkili hizmet sağlamaktadır. Bu durum, yalnızca müşteri deneyimini geliştirmekle kalmamakta, aynı zamanda havacılık endüstrisinde standardizasyonu, güveni ve paydaşlar arası tutarlılığı güçlendirmektedir (Ullah, 2025).

Sonuç olarak, Proje 777 ve Proje 321, havacılık sektörünü güvenli, verimli ve şeffaf bir dijital kimlik yönetimi modeline taşımakta; yapay zekâ destekli dijital dönüşümün havacılığın geleceğinde insan, teknoloji ve güvenlik arasında yeni bir denge kuracağını göstermektedir.

6.Türkiye’de Uygulama

Türkiye’de yapay zekâ destekli dijital kimlik uygulamaları, küresel havacılık trendleriyle paralel biçimde gelişmektedir. İstanbul Havalimanı ve Türk Hava Yolları iş birliğiyle Star Alliance’ın biyometri altyapısının test edilmesinin ardından, Miles & Smiles üyesi yolcular biyometrik geçiş sistemini aktif biçimde kullanmaya başlamıştır. Bu sistem sayesinde yolcular, yüz tanıma ve parmak izi doğrulaması yaptıktan sonra ortalama 18 saniye içinde 30 adet hızlı pasaport noktasından geçiş yapabilmektedir. Böylece İstanbul Havalimanı, biyometrik ve hızlı pasaport geçiş sistemini etkin ve yaygın bir biçimde uygulayan havalimanları arasında yer almıştır (istairport.com, 2025).

Türkiye’deki sistemde biyometrik veriler merkezi bir kimlik doğrulama veri tabanında tutulmamakta, yalnızca pasaport çipindeki bilgilerle eşleşme doğrulaması yapılmaktadır. Doğrulama işlemi tamamlandıktan sonra veriler geçici bellekte silinmektedir. Bu yapı, Türkiye Cumhuriyeti Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında düzenlenmiş olup, sistemin tüm veri güvenliği süreçleri yerel mevzuata uygun biçimde yürütülmektedir (Kişisel Verileri Koruma Kanunu [KVKK], 2016). İzmir Adnan Menderes Havalimanı’nda da hızlı pasaport sistemi aktif durumdadır. Yolcular çipli pasaportlarını, yüz tanıma ve parmak izi doğrulama işlemleriyle eşleştirerek dört hızlı geçiş bankosundan kolayca geçebilmektedir. Türk Hava Yolları, İzmir Havalimanı’nda biniş süreçlerinin de biyometrik yüz tanıma teknolojisiyle gerçekleştirilmesi için yeni bir sistem kurulum süreci planlamaktadır (izmirairport.com, 2025).

Türk Hava Yolları’nın yapay zekâ girişimleri günümüzde altmıştan fazla aktif modeli kapsamaktadır ve iki yüzden fazla çalışan doğrudan yapay zekâ tabanlı projelerde görev almaktadır. Şirket, açık kaynak tabanlı yapay zekâ platformu için Red Hat altyapısını tercih ederek bilet satışlarında daha isabetli dinamik fiyatlandırma uygulamalarıyla operasyonel verimliliği artırmayı hedeflemektedir.

Ayrıca müşteri kart ödemeleri ve Miles & Smiles sadakat programı işlemleri, dolandırıcılık tespiti amacıyla geliştirilen ileri düzey yapay zekâ modelleriyle taranmaktadır. Bu modeller, işlemlerdeki anormallikleri yüksek doğrulukla belirleyerek finansal güvenliği güçlendirmektedir. Operasyonel düzeyde ise uçuş rotaları, uçak özellikleri ve yakıt tüketimi gibi parametreleri dikkate alan atama optimizasyon modelleri kullanılmaktadır. Bu sayede her rota için en uygun uçak tipi seçilmekte, bu da yakıt tüketiminde önemli oranda tasarruf sağlamaktadır.

Ayrıca Türk Hava Yolları, operasyonel süreçlerin kesintisiz ilerlemesi için yer planı öngörülere, blok zaman analizi ve zamanında performans tahminleri gibi alanlarda yapay zekâ tabanlı iyileştirmeler gerçekleştirmektedir. Bu yaklaşımla tüm operasyonel birimler olası gecikmeler karşısında proaktif biçimde hareket etmekte, aksamalar en aza indirilmektedir (RedHat, 2025). Sonuç olarak, Türkiye’de dijital kimlik ve yapay zekâ uygulamaları hem yolcu deneyimini hızlandıran hem de operasyonel verimliliği artıran bir ekosisteme dönüşmüştür. İstanbul ve İzmir örnekleri, Türkiye’nin biyometri temelli dijital kimlik doğrulama sistemlerinde bölgesel lider olma potansiyelini güçlendirmektedir.

7. Sonuç ve Tartışma

Havacılık sektörü, yapay zekâ ve dijital kimlik teknolojilerinin birleşimiyle köklü bir dönüşüm sürecinden geçmektedir. IATA'nın öncülüğünde geliştirilen Proje 777 ve Proje 321, bu dönüşümün yalnızca teknik bir yenilik olmadığını, aynı zamanda güvenlik, yönetim ve etik anlayışında yeni bir dönemi başlattığını göstermektedir. Her iki proje de dijital kimlik doğrulama, biyometrik tanıma, veri gizliliği ve yapay zekâ destekli karar sistemlerinin entegre biçimde nasıl çalışabileceğine dair güçlü örnekler sunmaktadır. Kimlik doğrulama süreçlerinin artık günler yerine saniyeler içinde tamamlanabilmesi, operasyonel verimliliğin ve yolcu memnuniyetinin önemli ölçüde artmasını sağlamıştır.

Yapay zekânın veri analizi, risk tespiti ve biyometrik doğrulama alanlarındaki kullanımı, güvenlik açıklarının azaltılmasına ve karar destek sistemlerinin doğruluk ile hızının artmasına katkı sağlamaktadır. Süreçlerde insan hatasının azalması, havacılıkta emniyet kültürünün güçlenmesine ve operasyonel standartların tutarlılıkla uygulanmasına yardımcı olmaktadır.

Bununla birlikte, dijital dönüşüm beraberinde etik ve şeffaflık temelli yeni tartışmalar getirmiştir. Proje 777'de çalışan verilerinin sürekli izlenebilmesi, Proje 321'de ise biyometrik verilerin değiştirilemez niteliği, mahremiyet ve veri yönetimi konularında net düzenlemelere duyulan ihtiyacı açık biçimde ortaya koymaktadır. Yapay zekâ sistemlerinin karar verme süreçlerinin tam olarak açıklanamaması, hesap verebilirlik, adalet ve eşitlik ilkeleri açısından dikkatle ele alınması gereken bir konudur. Uzun vadede bu sistemlerin başarısı, uluslararası düzenleyici çerçevelerle uyum içinde geliştirilecek etik denetim mekanizmalarına bağlıdır. Bu nedenle etik gözetim, şeffaflık ve sorumluluk ilkeleri, teknolojik sürdürülebilirliğin temel bir bileşeni hâline gelmelidir.

Türkiye'de İstanbul Havalimanı ve Türk Hava Yolları örneklerinde görüldüğü gibi dijital kimlik ve biyometrik sistemlerin başarıyla uygulanması, ülkenin küresel havacılık standartlarına hızla uyum sağladığını göstermektedir. Bu uygulamalar hem yolcu deneyimini kolaylaştırmakta hem de güvenlik ve operasyonel emniyetin güçlenmesine katkıda bulunmaktadır. Yakın gelecekte "Tek Kimlik – Tek Seyahat" vizyonunun uluslararası düzeyde hayata geçirilmesiyle, seyahat süreçlerinin daha güvenli, hızlı ve temassız bir yapıya kavuşması beklenmektedir. Yapay zekânın insanın yerini tamamen alması öngörülmemekle birlikte, bu sistemlerin insanla iş birliği içinde ilerleyeceği öngörülmektedir. Kritik karar alma süreçlerinde insanın sezgisel değerlendirmesi ve sorumluluk bilinci hâlâ temel önemdedir. Yapay zekânın kendi kendini geliştirme kapasitesi sınırlı olsa da zamanla olgunlaşarak

daha güvenilir hâle gelecektir. Ancak bu gelişim, insan denetimi ve etik yönetiminden bağımsız gerçekleşmemelidir.

Sonuç olarak, yapay zekâ destekli dijital kimlik yönetimi, havacılık sektörünün geleceğini şekillendiren en önemli yeniliklerden biri olarak değerlendirilmektedir. Bu sistemlerin uzun vadeli başarısı, yalnızca dijital dönüşüme değil, aynı zamanda etik hesap verebilirlik, kurumsal şeffaflık, veri gizliliği ve insan merkezli tasarım ilkelerine bağlıdır. Geleceğin havacılığı, yapay zekânın hesaplama gücüyle insan sezgisinin dengeli biçimde birleştiği, güvenilir, şeffaf ve insana duyarlı bir ekosistem üzerine inşa edilecektir.

Havayolu sektörü, dijital kimlik uygulamalarından yararlanmak için büyük bir potansiyele sahiptir. Yapay zekâ algoritmaları, havacılıkta yalnızca dijital kimlik çözümleriyle sınırlı kalmayacak; güvenliği, verimliliği ve karar süreçlerini destekleyici bir unsur olarak her alanda kullanılmaya başlanacaktır. Bu kapsamda, sektörde dijital çalışan kimliği için ortak bir şema geliştirilebilir. Kimlik tabanlı otomatik giriş rehberleri hazırlanarak küresel bir dijital kimlik çerçevesi oluşturulabilir. Yakın gelecekte, biyometrik veriler de dâhil olmak üzere tüm elektronik kimlik bilgilerinin tek bir platformda güvenli ve şeffaf biçimde saklanması sağlayacak bir güven kayıt sistemi kurulabilir. Havalimanları için biyometrik uyum rehberlerinin geliştirilmesi, uygulama birliğini ve güvenilirliği artıracaktır.

Dijital cüzdana kimliğin yalnızca bir kez yüklenmesi yeterli olacağından, bu sistem farklı havalimanlarında kullanıcı deneyimi test edilerek sürekli iyileştirilebilir. Böylece yolcular, her noktada hızlı ve zahmetsiz bir şekilde kimlik doğrulaması yapabilir. Kurumsal iş birliği anlaşmalarında dijital çalışan kimliği dijital cüzdanla entegre edilerek, müşterilerin hem kimlik hem de sadakat programı verilerine 7/24 erişim sağlaması mümkün olacaktır. Bu süreç, kullanıcı hikâyeleri ve sade kılavuzlarla desteklenerek, dijital kimliğin günlük operasyonlara nasıl kolaylık sağladığı açık biçimde gösterilebilir.

Devlet ve özel sektör tarafından sağlanacak dijital cüzdan entegrasyonlarının teşvik edilmesi, sistemin yaygınlaşmasını hızlandıracaktır. Dijital kimlik kullanan yolculara veya çalışanlara yönelik teşvik mekanizmaları oluşturularak, daha fazla bireyin bu sisteme katılımı sağlanabilir. Bununla birlikte devletler ve özel sektör kuruluşları arasında kimlik tanıma ve doğrulama konusunda karşılıklı mutabakatlar yapılabilir. Dijital kimliklerin başarılı biçimde hayata geçirilebilmesi için hukuki ve düzenleyici çerçevelerin güncellenmesi ve yapay zekâ destekli süreçlerin etik ilkelere uygun biçimde denetlenmesi gerekmektedir. Bu adımların atılması, yolcunun “tek kimlik- tek seyahat” deneyimini küresel ölçekte mümkün kılacak; havacılık sektörünü güvenli, şeffaf ve bütünleşik bir dijital kimlik ekosistemine taşıyacaktır.

Kaynakça

- Abudureyimu, Y., ve Oğurlu, Y. (2021). Problems and solution proposals that artificial intelligence applications may cause regarding the protection of personal data. *Journal of Social Sciences of Istanbul Commerce University*, 20(40), 765–782.
- AI & EUROCONTROL. (2020, March). Using biometrics to accelerate secure boarding (FLY AI Report). *EUROCONTROL and European Aviation High Level Group On AI* <https://www.eurocontrol.int/sites/default/files/2020-03/eurocontrol-fly-ai-report-032020.pdf>, Erişim Tarihi: 11.12.2025.
- Alanazi, M. S. M., Li, J., ve Jenkins, K. W. (2024). Evaluating Airport Service Quality Based on the Statistical and Predictive Analysis of Skytrax Passenger Reviews. *Applied Sciences*, 14(20), 9472. <https://doi.org/10.3390/app14209472>, Erişim Tarihi: 11.11.2025.
- Alshamaileh, L. (2023). *The use of biometric systems in critical infrastructures and their role in cybersecurity: Aviation industry focused* [Yayımlanmamış doktora tezi]. Doctoral School of Safety and Security Sciences <https://exampleuniversityrepository.edu/thesis/alshamaileh2023>, Erişim Tarihi: 10.12.2024.
- Alshurideh, M., Alsharari, N., & Al Kurdi, B. (2019). *Supply chain integration and customer relationship management in the airline logistics. Theoretical Economics Letters*, 9(2), 392–414. <https://doi.org/10.4236/tel.2019.92029>, Erişim Tarihi: 08.11.2025.
- Blokchain Türkiye Platformu BCTR. (2025, September 23). Dijital kimlik sistemleri ve sektörel etkiler. *Türkiye Bilişim Vakfı – Blockchain Türkiye Platformu*. <https://bctr.org>, Erişim Tarihi: 07.11.2025.
- Bullchand-Gidumal, J. G. (2020). Impact of artificial intelligence in travel, tourism, and hospitality. *Institute for Sustainable Tourism and Economic Development (TIDES)*, University of Las Palmas de Gran Canaria. https://acceda.cris.ulpgc.es/bitstream/10553/106011/2/impact_artificial_intelligence.pdf, Erişim Tarihi: 13.11.2025.
- Çevik, N., ve Akleylek, S. (2022). Havacılık sistemlerinde siber güvenlik. Ş. Sağiroğlu, S Akleylek (Ed.) *Siber Güvenlik ve Savunma Kitap Serisi 6: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler* içinde (s. 293-324) 1. Basım Haziran İstanbul: Nobel Yayıncılık.
- Doğan, Ö., ve Karacan, H. (2022). Türkiye’deki e-ticarete özgü blokzincir tabanlı dijital kimlik güven çerçevesi önerisi. *Bilgi Yönetimi Dergisi*, 5(2), 256–279. <https://doi.org/10.33721/by.1113558>, Erişim Tarihi: 11.10.2025.
- ECAT. (2024, November 27). European Centre for Algorithmic Transparency. European Commission. <https://ec.europa.eu/ecat>, Erişim Tarihi: 13.10.2025.
- Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assess-

- ment. IEEE Access, 9, 143997-144016. <https://doi.org/10.1109/ACCESS.2021.3121230>, Erişim Tarihi:09.12.2025.
- European Commission. (2023). European digital identity framework (eIDAS 2.0). *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>, Erişim Tarihi:11.11.2025.
- European Union. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*.
- European Union. (2018). General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, Erişim Tarihi:12.11.2025.
- Farrow, E. (2019). To augment human capacity — *Artificial intelligence evolution*. *AI Review*, 61, 45–58.
- Future Travel Experience. (2023, January). Istanbul Airport and Turkish Airlines test Star Alliance biometrics access system. <https://www.futuretravelexperience.com/2023/01/istanbul-airport-and-turkish-airlines-test-star-alliance-biometrics-access-system>, Erişim tarihi:12.11.2025.
- International Air Transport Association. (2025a). Exploring artificial intelligence and digital identity use cases in aviation: Project 777 / Project 321 (pp. 12–32). International Air Transport Association,
- International Air Transport Association. (2025b). Annual review *International Air Transport Association*. (pp. 1-58). <https://www.iata.org/en/programs/innovation/digital-identity>, Erişim Tarihi:04.11.2025.
- International Civil Aviation Organization. (2013). Aviation security manual (Doc. 9985). *International Civil Aviation Organization*. <https://elibrary.icao.in>, Erişim Tarihi:08.12.2025.
- International Civil Aviation Organization. (2016, July). Safety management (Annex 19). *International Civil Aviation Organization*. <https://caainternational.com/>, Erişim Tarihi:07.11.2025.
- International Civil Aviation Organization. (2019). Doc 9303 – Machine readable travel documents. Montreal, Canada: *International Civil Aviation Organization*.
- International Civil Aviation Organization. (2025, September 27). The impact of artificial intelligence on the aviation sector: Innovation in aviation (Agenda Item 20, Assembly 42, Session EX/168). *International Civil Aviation Organization*.
- International Civil Aviation Organization. (2025, September 27). The impact of artificial intelligence on the aviation sector: Innovation in aviation (Agen-

- da Item 20, Assembly 42, Session EX/168). *International Civil Aviation Organization*
- İGA. (2024). Biometrik geçiş ve dijital kimlik uygulamaları. <https://www.istairport.com/hizmetler/deneyim/havalimani-hizmetleri/hizli-pasaport-gecis>, Erişim Tarihi: 16.12.2025.
- İstanbul Airport. (2025, October 23). [istairport.com](https://www.istairport.com). <https://www.istairport.com>, Erişim Tarihi: 09.12.2025.
- İzmir Airport. (2025, October 19). [izmirairport.com](https://www.izmirairport.com). <https://www.izmirairport.com>, Erişim Tarihi: 09.12.2025.
- Jiang, X., Zhang, Y., ve Li, Y. (2022 July 01). Forecast and analysis of aircraft passenger satisfaction based on RF-RFE-LR model. *Sci Rep* 12, 11174 <https://doi.org/10.1038/s41598-022-14566-3>
- Jiang, Y., Tran, T. H., ve Williams, L. (2023). Machine learning and mixed reality for smart aviation: Applications and challenges. *Journal of Air Transport Management*, 111, 1–16. <https://doi.org/10.1016/j.jairtraman.2023.102437>, Erişim Tarihi: 01.11.2025.
- Kişisel Verileri Koruma Kurumu (KVKK). (2016, March 24). [kvkk.gov.tr](http://www.kvkk.gov.tr). <http://www.kvkk.gov.tr>, Erişim Tarihi: 20.11.2025.
- Meydan, C. H. (2023, February). Havayolu işletmelerinde dijital dönüşüm uygulamaları üzerine bir inceleme. *Journal of Aviation Research*, 5(1), 65–82.
- Noah, A., Moon, L., ve John, A. (2024, December). The consequences of non-compliance with data protection regulations on business analytics. *Business Analytics Review*, 12(4), 233–245. <https://www.researchgate.net/publication/386409782>, Erişim Tarihi: 15.11.2025
- Red Hat. (2025). Turkish Airlines pioneers AI-led innovation for aviation with Red Hat OpenShift AI. <https://www.redhat.com>, Erişim Tarihi: 12.12.2025.
- Sing, P. K. B. (2025). Data-driven catering services: Reducing food waste and maximizing profit. *Airline Customer Experience* içinde (ISBN 9781003625100).
- Singh, R. P., Javaid, M., Haleem, A., ve Suman, R. (2020). Internet of Things (IoT) applications to fight against COVID-19 pandemic. *Diabetes & Metabolic Syndrome*, 14(4), 521–524. <https://doi.org/10.1016/j.dsx.2020.04.041>, Erişim Tarihi: 14.12.2025.
- Şahan, D. (2025). Hava kargo endüstrisinde dijitalleşme: IATA programları üzerine bir vaka çalışması. *İzmir Yönetim Dergisi*, 6, 160–173. <https://doi.org/10.56203/iyd.1668548>, Erişim Tarihi: 12.12.2025.
- Takçı, H. (2020). Saldırı tespit sistemleri ve log (günlük) analizi. Sağıroğlu, S. Akleyek (Eds.), *Siber Güvenlik ve Savunma: Biyometrik ve Kriptografik Uygulamalar* içinde (s. 29–53). Ankara: Nobel Yayıncılık.

- Ullah, A. (2025). The effect of artificial intelligence (AI) on customer experience. *Science PG Journal of Technology and Science*, 13(2), 54–60. <https://doi.org/10.11648/j.ijsts.2025.13.02.13>, Eriřim Tarihi:09.12.2025.
- Ünal, G., ve Uluyol, Ç. (2020, Nisan). Blok zinciri teknolojisi. *Biliřim Teknolojileri Dergisi*, 13(2), 56–65. <https://doi.org/10.17671/gazibtd.542417>, Eriřim Tarihi:20.11.2025.
- Windley, P. J. (2005). Digital identity: Unmasking identity management architecture. O'Reilly Media Inc. ISBN: 0-596-00875-3