Yönetim Bilişim Sistemleri Derneği Dergisi

Cilt:2 | Sayı:1 | 2026

ISSN: 3108-6454

YBS

Yönetim Bilişim Sistemleri Derneği

Journal of Management Information Systems Association

https://www.ybs.org.tr/ybsdd

YÖNETİM BİLİŞİM SİSTEMLERİ DERNEĞİ DERGİSİ

Journal of Management Information Systems Association

Cilt/Volume: 2

Sayı/Issue: 1

Yıl/Year: 2026

Yönetim Bilişim Sistemleri Derneği Yayınevi

İzmir – 2026

Journal of Management Information Systems Association

Cilt/Volume: 2 Sayı/Issue: 1 Yıl/Year: 2026

Yönetim Bilişim Sistemleri Derneği Dergisi (YBSDD), Yönetim Bilişim Sistemleri Derneği bünyesinde Haziran ve Aralık aylarında yılda iki kere çevrim içi olarak yayımlanan hakemli ve süreli bir dergidir. Derginin yayın dili Türkçe ve İngilizce'dir. Dergide yayımlanan çalışmalara ilişkin olarak yazarlara ödeme yapılmamakta ve yazarlardan makale gönderimi, editörlük süreçleri, yayın ücreti gibi hiçbir ad altında ücret talep edilmemektedir. Dergide yer alan yazıların sorumluluğu yazarlarına aittir. Dergide yer alan yazılar kaynak gösterilmeksizin alıntılanamaz.

Yayımcı/Publisher
Yönetim Bilişim Sistemleri Derneği

Adres/Address: Yalı Mah. Mithatpaşa Cad. Dış Kapı No:341 İç Kapı No: 1, Güzelbahçe/İzmir/Türkiye
E-Posta/E-Mail: ybsdd@ybs.org.tr
Web Sitesi/Web Site: www.ybs.org.tr/ybsdd

İÇİNDEKİLER/CONTENTS

Cilt: 2, Sayı: 1, 2026, Sayfa: 1-26

Yönetim Bilişim Sistemleri Derneği Dergisi

ISSN: 3108-6454

Journal of Management Information Systems Association

https://www.ybs.org.tr

LLM DESTEKLİ BİR MOBİL YOKLAMA ASİSTANI – BURSA ULUDAĞ ÜNİVERSİTESİ ÖRNEĞİ

Fatma SERT[a] ve Erdal ÖZDOĞAN[b]

Makale Bilgisi

Makale Türü
Araştırma Makalesi

Gönderim Tarihi:
21/04/2026

Kabul Tarihi:
22/06/2026

Anahtar Kelimeler:
Akıllı Yoklama, QR Tabanlı Yoklama, Proaktif Yoklama Sistemi, LLM destekli yoklama, Bağlam Duyarlı Yoklama.

Özet

Geleneksel yoklama sistemleri genellikle öğrenci bağlılığını ve veri erişilebilirliğini göz ardı ederek yalnızca kayıt tutmaya odaklanmaktadır. Bu çalışma, yoklama sürecini durağan bir idari görevden bir akademik asistana dönüştüren, bir mobil yoklama ekosistemi sunmaktadır. Sistem, dinamik QR kod tarama ile desteklenen çok katmanlı bir doğrulama çerçevesi kullanarak güvenli, hızlı ve yakınlık tabanlı bir doğrulama süreci sağlar. Coğrafi sınırlama ile bu hibrit kontrol mekanizmalarını birleştiren sistem; akademik motivasyonu ve zaman yönetimini artırmak amacıyla, öğrencilere kampüse giriş yaptıklarında kişiselleştirilmiş dijital dürtme ve ders programı hatırlatıcıları sunarak bağlam duyarlı etkileşimler başlatır. Önerilen mimari, eğitmenlerin doğal dil sorguları aracılığıyla veri analizleri yapmasına sağlayan bir LLM katmanı entegre etmektedir. Böylece devamsızlık sınırını aşma riski taşıyan öğrencilerin önceden belirlenmesi gibi gerçek zamanlı müdahalelere imkân tanır. Ayrıca sistem, BYOD modelini benimseyerek veri gizliliğine ve maliyet etkinliğine öncelik verir. Bu sayede pahalı biyometrik donanım veya sabit altyapı kurulumlarına duyulan ihtiyacı ortadan kaldırır.

[a] Bursa Uludağ Üniversitesi, İnegöl İşletme Fakültesi, Yönetim Bilişim Sistemleri Bölümü, Bursa ORCID: 0009-0000-4346-5519

[b] Bursa Uludağ Üniversitesi, İnegöl İşletme Fakültesi, Yönetim Bilişim Sistemleri Bölümü, Bilişim Sistemleri ABD., 16400 Bursa, ORCID: 0000-0002-3339-0493

LLM-POWERED MOBILE ATTENDANCE ASSISTANT: A CASE STUDY OF BURSA ULUDAĞ UNIVERSITY

Article Information

Article Type
Research Article

Submission Date:
21/04/2026

Acceptance Date:
22/06/2026

Keywords: Smart Attendance, QR-Based Attendance, Proactive Attendance System, LLM-Powered Attendance, Context-Aware Attendance

Abstract

Traditional attendance systems often focus solely on record-keeping, neglecting student engagement and data accessibility. This study presents a mobile attendance ecosystem that transforms the attendance process from a static administrative task into an academic assistant. The system provides a secure, rapid, and proximity-based verification process using a multi-layered authentication framework supported by dynamic QR code scanning. Integrating these hybrid control mechanisms with geofencing, the system initiates context-aware interactions—such as personalized digital nudges and schedule reminders when students enter the campus—to enhance academic motivation and time management. The proposed architecture integrates an LLM layer that enables instructors to perform data analysis through natural language queries, allowing for real-time interventions, such as the early identification of students at risk of exceeding absence limits. Furthermore, the system prioritizes data privacy and cost-effectiveness by adopting the BYOD model, thereby eliminating the need for expensive biometric hardware or fixed infrastructure installations.

1. GİRİŞ

Yükseköğretim kurumlarında öğrenci başarısının ve akademik performansın temel belirleyicilerinden biri derslere düzenli katılımdır (Yilmaz vd., 2020; Dalkılıç ve Aydın, 2018). Üniversite eğitimi, sadece bilgi aktarımı değil, aynı zamanda sosyal etkileşim ve eleştirel düşünme becerilerinin kazanıldığı bir süreçtir. Bu bağlamda derse devamlılık, öğrencinin müfredata uyum sağlaması ve kurumsal aidiyet duygusunu geliştirmesi açısından kritik bir öneme sahiptir (Aynas, 2024). Bilişim teknolojilerindeki gelişmeler, eğitim süreçlerinin dijitalleşmesini sağlarken, bu dönüşüme paralel olarak devam kontrol süreçleri de gelişimini sürdürmektedir. Nitekim devam takip sistemlerin geleneksel yöntemlerden başlayıp, biyometrik yöntemlere, ardından Radyo Frekansı ile Tanımlama (RFID) tabanlı çözümlerden Nesnelerin İnterneti (IoT) tabanlı çözümlere doğru evrim geçirdiği söylenebilir (Salunkhe vd., 2025). Yapılan araştırmalar, özellikle Yapay Zekanın idari verimliliği artırdığını, kişiselleştirilmiş öğrenme yolları sunduğunu ve yenilik yönetiminin okullarda kritik bir ihtiyaç haline geldiğini ortaya koymaktadır (Cankurtaran, 2025). Eğitimde birçok alanda olduğu gibi devam takibinde de YZ ve Makine Öğrenmesi gibi dijital yöntemlere dayalı akıllı yoklama sistemleri kullanılmaktadır. Öte yandan, dijitalleşen bu süreçlerde biyometrik verilerin dikkat, stres ve katılımı izlemede nesnel kanıtlar sunduğu görülmekte, ancak bu verilerin "özel nitelikli kişisel veri" statüsünde olması nedeniyle Kişisel Verileri Koruma Kanunu (KVKK) kapsamında sıkı bir şekilde korunması gerektiği gerçeği unutulmamalıdır (Şılbır, 2025). Buna karşın, literatür incelendiğinde akıllı yoklama sistemlerine yönelik araştırmaların %90'ından fazlasının teknik performans ve güvenliğe odaklandığı, etik kaygıların ise neredeyse hiç yer

almadığı dikkat çekmektedir (Purnamawati vd., 2026). Dolayısıyla teknolojik araçların varlığı, tek başına eğitimin kalitesini ve öğrenci başarısını artırmak için yeterli değildir. Bu noktada önemli olan hem hukuki sınırlara sadık kalıp hem de bu verilerin nasıl anlamlandırıldığı ve eğitsel bir değere nasıl dönüştürüldüğüdür. Tam da bu noktada Büyük Dil Modelleri (LLM), toplanan devamsızlık ve katılım verilerini analiz ederek akademik risk altındaki öğrencileri erkenden tespit etme, öğretim elemanlarına otomatik/anlamlı raporlar sunma ve öğrencilere kişiselleştirilmiş eğitsel geri bildirimler üretme gibi benzersiz avantajlar sağlamaktadır.

LLM'ler, verinin sadece kaydedilmesinden ziyade, verinin analiz edilmesi ve anlamlandırılması aşamasında kritik bir rol oynar (Neelakantan vd., 2025). LLM destekli sistemler öğrencilere, öğretim görevlilerine ve yöneticilere çeşitli avantajlar sunmayı hedefler. Yöneticilerin karmaşık sorgular yazmak yerine, "Bugün hangi bölümün katılımı %80'in altında?" gibi doğal dilde sorular sorarak veritabanından istatistiksel bilgi almasını sağlar (Yugesh vd., 2024). Benzer şekilde öğrencilerin devam verilerini analiz ederek kategoriler oluşturma ve buna göre kişiselleştirilmiş çalışma tavsiyeleri sunma yetenekleri bulunmaktadır (Chilakala vd., 2026). Ek olarak derse katılımı azalan veya akademik olarak geri düşme riski olan öğrencileri, yoklama ve diğer etkileşim verilerini birleştirerek tahminleme yapma ve öğretim görevlilerine erken uyarı gönderme gibi oldukça faydalı uygulama geliştirme potansiyeli sunmaktadır (Basit, vd., 2025).

1.1 Problem Durumu

Günümüzün kalabalık sınıflarında ve dinamik eğitim yapısında, devam takibini geleneksel yöntemlerle yönetmek hem etik hem de operasyonel açıdan bazı sorunları beraberinde getirmektedir (Uçar ve Uludağ, 2018; Pehlivanoğlu ve Duru, 2016; Akçay ve Altay, 2023; Uğuz ve Turan, 2020; Sezdi ve Tüysüz, 2018). Mevcut kullanılan sistemlerin ortak sorunu reaktif bir yapıda olmalarıdır. Yani devamsızlık olayı gerçekleşip veri üretildikten sonra sistem devreye girmektedir. Bu nedenle geleneksel çözümler, öğrenci motivasyonu ve kampüs aidiyeti gibi bütüncül eğitsel kazanımları sürece entegre etme noktasında kısıtlı bir etki alanına sahiptir.

Bilişim teknolojilerindeki ilerlemelerle birlikte, geleneksel imza yöntemlerine alternatif olarak kartlı geçiş sistemleri, biyometrik tarayıcılar ve QR kod tabanlı çeşitli dijital devam sistemleri geliştirilmiştir. Teknoloji geliştikçe bu araçlar daha işlevsel hale gelmiş olsa da mevcut çözümlerin çoğu halen bazı temel eksiklikler barındırmakta veya tamamlayıcı özelliklerden yoksun kalmaktadır. Örneğin, biyometrik tabanlı sistemler yüksek kurulum maliyetleri ve KVKK konusundaki hassasiyetler nedeniyle her kurumda kolayca uygulanamamaktadır. Kartlı sistemler, kartın bir başkasına verilmesi gibi suistimallere açık yapısını korurken, QR kod tabanlı çözümler ise öğrencilerin kodun fotoğrafını birbirine göndermesi gibi güvenlik açıklarına yol açabilmektedir. Ayrıca, mevcut sistemlerin çoğu sadece veri toplama odaklı olup öğrenciyle etkileşim kurmayan statik yapıları nedeniyle bütüncül bir çözüm sunmaktan uzaktır.

Mevcut literatür incelendiğinde, akıllı devam kontrol sistemlerinin genellikle maliyet, etkileşim eksikliği ve verilerin analiz süreci olmak üzere üç ana eksende tıkandığı görülmektedir. Öte taraftan, eğitici ve öğrenciler, parmak izi yöntemiyle yapılan devam kontrol uygulamasının derslere olan ilgi ve ders başarısı üzerinde olumlu bir etkisinin olmadığını düşünmektedirler (Bahşi vd., 2018). Yine mevcut uygulamalar öğrenciyle sadece yoklama anında etkileşime girmekte, öğrencinin kampüs içindeki hareketini bir akademik fırsata dönüştürememektedir. Benzer şekilde toplanan verinin anlamlandırılması ve yapılandırılması süreci, idari personel için zaman alıcı ve hataya meyilli olabilir. Literatürde, idari veya akademik görevdeki son kullanıcıya Doğal Dil İşleme (NLP/LLM) aracılığıyla doğrudan analiz sunan bir sistem eksikliği açıkça görülmektedir. Bu eksiklikler ve suistimal riskleri, daha ekonomik, güvenli ve öğrenci merkezli yeni nesil bir sistem ihtiyacını doğurmuştur.

1.2 Temel Katkılar

Bu çalışma kapsamında tasarlanan sistem, yalnızca geleneksel yoklama verilerini dijitalleştirmekle kalmayıp, mevcut çözümlerdeki yapısal zayıflıkları gidermeye yönelik tamamlayıcı özellikler içermektedir. Araştırmanın temel motivasyonu, teknolojik altyapıyı (dinamik QR, LLM entegrasyonu, mekân duyarlılığı) yalnızca veri kaydetmek için değil, yöneticiler, eğitmenler ve öğrenciler arasındaki iletişim boşluğunu kapatmak için kullanmaktır. Sistemin sağladığı diğer bir avantaj, veri güvenliği ve akademik dürüstlüğün düşük maliyetli bir altyapı ile sağlanmasıdır. Ek donanım yatırımı gerektirmeyen Kendi Cihazını Getir (BYOD) yaklaşımı sayesinde, eğitim süreçlerinde önemli bir sorun olan "yerine imza atma" gibi suistimaller minimize edilmektedir. Sistemin teknolojik mimarisi, dinamik ve konum duyarlı QR kod üzerine inşa edilmiştir. Bu yapı, öğrencinin fiziksel mevcudiyetini mekân ve zaman bağlamında yüksek doğrulukla teyit ederek yoklama sürecinin güvenilirliğini üst seviyeye çıkarmaktadır. Ayrıca, önerilen mimariye entegre edilen LLM katmanı, yöneticiler ve eğitmenler için veri analizi süreçlerini kolaylaştırmaktadır. Kullanıcılar, teknik bir raporlama arayüzüne ihtiyaç duymaksızın doğal dil sorguları aracılığıyla karmaşık veri setleri üzerinde analizler gerçekleştirebilmektedir. Bu sayede, devamsızlık verileri analiz edilerek akademik risk altındaki öğrenciler erkenden fark edilebilir, yapay zekâ desteğiyle ihtiyaç duyulan müdahaleler çok daha hızlı ve etkili bir şekilde gerçekleştirilebilir.

Sistemin sunduğu temel işlevlerden biri de öğrenci motivasyonu ve öz-denetim mekanizmasıdır. Öğrencilere devam durumlarına dair sistem tarafından gönderilen otomatik bilgilendirmeler, öğrencinin akademik sorumluluğunu hatırlatmakta ve devamsızlık sınırına dair riskleri erkenden görmesini sağlamaktadır. Sistem, kampüs sınırları içindeki öğrencilere anlık bildirimler aracılığıyla ulaşarak, henüz bir sorun yaşanmadan onlara destek sunan çift yönlü bir iletişim köprüsü görevi görmektedir. Bu yaklaşım, yoklama sistemlerini pasif birer denetim aracından, akademik başarıyı ve öğrenci motivasyonunu doğrudan etkileyen aktif bir öz-denetim mekanizmasına dönüştürür. Bu bağlam duyarlı etkileşimler, birer dijital dürtme işlevi görerek öğrencinin akademik sorumluluk bilincini pekiştirirken, aynı zamanda kurumla olan aidiyet bağını güçlendirmekte ve devamsızlık risklerine karşı erken uyarı

sağlayan bir öz-denetim mekanizması oluşturmaktadır. Bu tür bildirimler ve hatırlatıcılar, öğrencileri harekete geçirmek için zamanında ve kişiselleştirilmiş uyaranlar sağlar (Berger vd., 2025; Tate, 2023). Operasyonel açıdan ise sistem, dinamik süreç yönetimi imkânı tanımaktadır. Derslik değişikliği, zorunlu saat revizeleri ve ders erteleme gibi acil durumlarda öğrenciye gönderilen anlık bildirimler, iletişimi kesintisiz kılmaktadır. Ayrıca, ders programlarının ve sınav tarihlerinin otomatik olarak öğrenci takvimlerine entegre edilmesi, sistemi basit bir kayıt aracından çıkarıp destekleyici bir akademik asistan modeline dönüştürmektedir.

Bu çalışmanın literatürdeki uygulamalardan temel farkı ve özgün değeri, yoklama sürecini sadece bir denetim ve kayıt mekanizması olarak değil, öğrenciyle kurum arasında sürekli ve dinamik bir etkileşim kuran akıllı bir ekosistem olarak kurgulamasıdır. Mevcut sistemler genellikle pasif veri toplama ve raporlama odaklıyken, bu model, mekân duyarlı güvenli mimarisi ile veri manipülasyonu risklerini minimize ederken, eş zamanlı olarak LLM entegrasyonu ve otomatik bildirim mekanizmalarıyla öğrenci davranışlarına rehberlik eden bir akademik asistan rolü üstlenmektedir. Dolayısıyla önerilen sistem, yoklamayı geleneksel bir idari yük olmaktan çıkarıp, akademik başarıyı ve kurum aidiyetini destekleyen bir müdahale aracına dönüştürmesiyle özgün bir model sunmaktadır.

Önerilen sistem, farklı paydaşlar için çok katmanlı bir fayda modeli sunarak akademik süreçleri iyileştirmeyi hedeflemektedir. Eğitmenler ve yöneticiler için sistem, entegre LLM katmanı sayesinde karmaşık ya da dağıtık olan verileri teknik arayüzlere ihtiyaç duymadan, doğal dil sorgularıyla analiz etme imkânı tanımaktadır. Bu da akademik risk altındaki öğrencilerin erkenden tespit edilerek desteklenmesini sağlamaktadır. Öğrenciler için ise BYOD yaklaşımıyla, kişisel biyometrik verilerin paylaşılması endişesi olmadan güvenli bir katılım ortamı sunar. Anlık bildirimler aracılığıyla uygulanan dijital dürtme mekanizmaları sayesinde akademik sorumluluk bilinci pekiştirilmesi hedeflenir. Son olarak sistem, ders ve sınav süreçlerini öğrenci takvimiyle otomatik senkronize ederek, yoklamayı basit bir idari denetim aracı olmaktan çıkarmakta ve öğrencinin akademik başarısına katkı sunan bir akademik asistan modeline dönüştürmektedir.

Makalenin geri kalanı şöyle organize edilmiştir. İkinci bölümde alanda yapılmış çalışmalar incelenmiştir. Üçüncü bölümde önerilen sistem mimarisi ve çalışmanın metodolojisi sunulmuştur. Tartışma bölümünde alanda yapılan çalışmalardan elde edilen uygulama özellikleri ele alınmıştır. Sonuç bölümünde çalışma özetlenmiştir.

2. LİTERATÜR ÖZETİ

Literatürde yer alan akıllı yoklama sistemlerine dair çalışmalar incelendiğinde, araştırmaların büyük bir kısmının RFID ve biyometrik sensörler gibi donanım maliyeti gerektiren altyapılar üzerinden şekillendiği görülmektedir. Bu kapsamda 2018 yılında Uludağ ve Uçar tarafından yapılan bir çalışmada (Uçar ve Uludağ, 2018), eğitim kurumlarında geleneksel kâğıt tabanlı yoklama süreçlerinin neden olduğu zaman kaybını, karmaşıklığı ve sınav esnasındaki kimlik kontrolünün yarattığı dikkat

dağınıklığını ortadan kaldırma amaçlanmıştır. Çalışmada IoT teknolojileri kullanılarak, öğrenci devam takibinin e-imza mantığıyla dijitalleştirilmesi ve devam sınırındaki öğrencilerin otomatik e-posta yoluyla uyarılması hedeflenmiştir. Çalışmada donanım tabanlı RFID teknolojisi ve biyometrik parmak izi okuma sensörleri entegre edilmiştir. Aydın ve Dalkılıç (2018), RFID teknolojisinden yararlanarak öğrencilerin devam durumlarını izleyen temassız bir akıllı kart sistemi kurgulamışlardır. Araştırmacılar, geliştirilen bu donanım altyapısını desteklemek ve verilerin yönetimini kolaylaştırmak amacıyla web tabanlı bir takip arayüzü de tasarlamışlardır. Pehlivanoğlu ve Duru (2016) çalışmasında yine parmak izi okuyucu sistem tasarlanmış ve öğrenci devamının takip edilmesi amaçlanmıştır. Uğuz ve Turan (2020) akıllı telefon, internet bağlantısı ve elektrik kaynağına ihtiyaç duymayan, taşınabilir özellikli, parmak izi okumaya dayalı dijital bir öğrenci yoklama sistemi geliştirmişlerdir. Çalışmada sistemin web tabanlı bir uygulamasının yapılarak kampüs öğrenci bilgi sistemine entegre edilmesi, dokunmatik ekran eklenmesi, kapasitesi daha yüksek ve hassas sensörlerin kullanılması gerektiği vurgulanmıştır. Turan ve Doğan (2024) çalışmasında geleneksel yoklama yöntemlerinin yol açtığı zaman israfını ve yerine imza atma gibi sorunları önlemek amacıyla Yüz Tanıma Tabanlı Öğrenci Takip Sistemi geliştirilmiştir. Sezdi ve Tüysüz (2018) Fonksiyonel Elektronik Yoklama Sistemi adı verilen, kurumun halihazırda var olan elektronik bilgi sistemi ve mevcut kimlik kartlarını kullanan, web servis tabanlı ve RFID kartlı bir yoklama sistemi geliştirilmişlerdir. Yazarlar sistemin en büyük zafiyeti olarak, bir öğrencinin derse gelmeyen başka bir arkadaşının kartını okutarak sistemi yanıltabilmesi olduğunu belirtmişlerdir.

Akçay ve Altay (2023) çalışmasında Bluetooth düşük enerji (BLE) teknolojisine sahip işaret yayıcı cihazlar ve akıllı telefonlar kullanılarak, öğrencilerin derse katılım sürelerini saat bazında belirleyen bir yoklama otomasyonu geliştirmişlerdir. Yazarların önerdiği sistemde öğrenciler, çevredeki işaretçiyi aratır ve kendisine en yakın olanı seçerek öğrenci numarası ve şifresiyle sisteme giriş yapar. Bilen ve diğerlerinin (2015) çalışmasında öğrencinin GPS konum verisi kullanarak çalışan, K-En Yakın Komşu (KNN) algoritması tabanlı etkileşimli ve gerçek zamanlı bir mobil yoklama yazılımı geliştirilmiştir. Çalışmada öğrenci konum verisine en uygun dersi seçerek sisteme giriş yapmaktadır. Ancak her iki çalışmada da bu süreç öğrencilerin elle seçim yapması nedeniyle hataya meyillidir.

Ekincioğlu ve Keser (2025), sınıf içi video akışından yüz tespiti yapan ve SVM, CNN gibi modelleri çoğunluk oyu ile birleştiren hibrit bir yoklama sistemi geliştirerek küçük sınıflarda %97'ye varan yüksek doğruluk oranlarına ulaşmıştır. Küçük sınıflarda %97'ye varan yüksek doğruluk oranlarına ulaşan bu çalışma, sert ışık ve çok eğik yüz görünümleri gibi durumlarda hata payının arttığını belirtmiştir. Ancak söz konusu sistemin video tabanlı donanıma bağımlı olması ve bireysel görüntü mahremiyetine dair taşıdığı riskler, çalışmamızın odaklandığı BYOD yaklaşımından ile farklılaşmaktadır.

Ege ve Özdemir (2026), ağırlık sensörleri ve RFID modülleri kullanarak donanım tabanlı bir yoklama sistemi geliştirmiştir. Benzer bir çalışmada Özcan ve diğerleri (2018), mobil cihazlar için RFID ve Bluetooth Düşük Enerji (BLE) teknolojisini kullanan bir yoklama uygulaması geliştirmiştir. Polat ve Doğan (2025), Raspberry Pi 4 ve OpenCV kütüphanesini kullanarak, LBPH algoritması tabanlı düşük

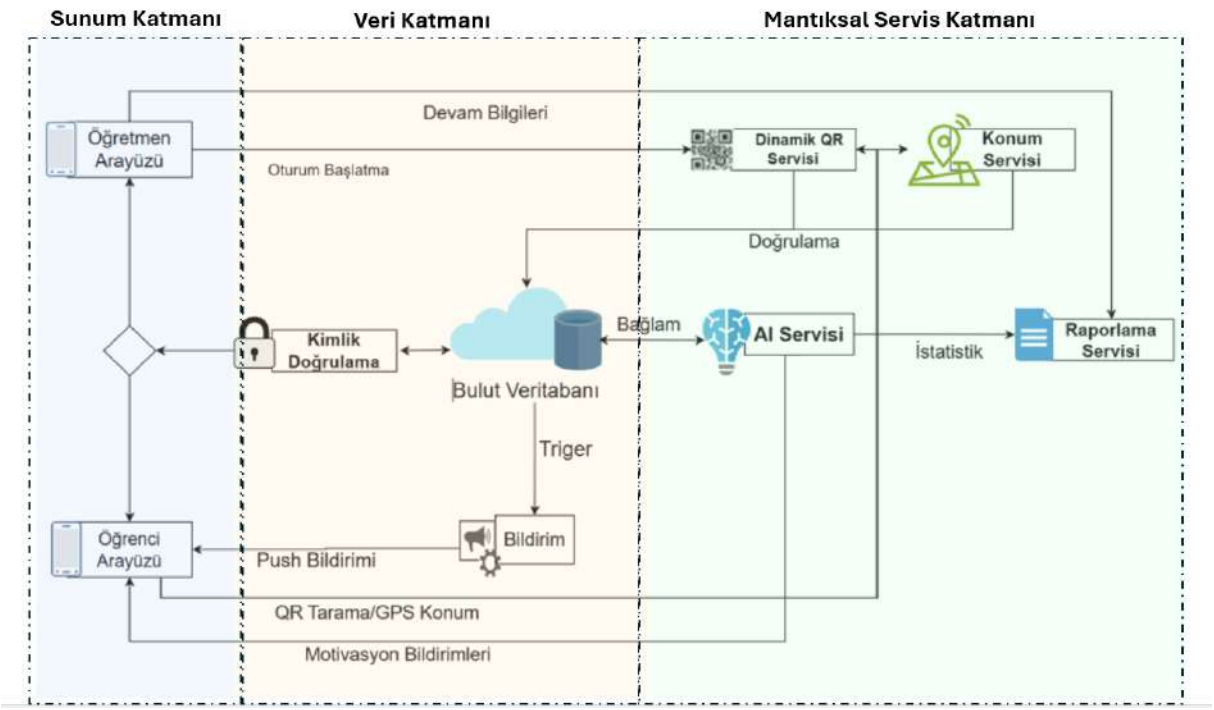
maliyetli ve taşınabilir bir yüz tanıma sistemi geliştirmiştir. Beş öğrenci üzerinde yapılan testlerde %92,5 doğruluk oranına ve 0,15 saniyelik hızlı tanıma süresine ulaşmışlardır. Ancak her üç çözüm de fiziksel kurulum ve yüksek maliyetli donanım bağımlılığına neden olmaktadır.

Çalışmamıza benzer olarak 2024 yılında yapılan güncel bir çalışmada, LLM destekli devam yönetim ve analiz sistemi tasarlanmıştır. Web tabanlı çalışan bu sistemde öğrenciler için Chatbot özelliği eklenmiştir. Yazarlar duyuru modülü ve haber modülünün bu tür sistemlere entegre edilmesini önermişlerdir (Yugesh vd., 2024). Çalışmamız mobil uygulama olması nedeniyle daha kullanışlı olması ve belirtilen ek özellikleri de içermesi yönünden ayrışmaktadır. LLM kullanımı yönünden çalışmamıza oldukça benzer diğer bir çalışmada, öğrencilerin akademik ve idari bilgilere erişimini kolaylaştırmak amacıyla LLM ile güçlendirilmiş NexU adlı akıllı bir kampüs asistanı geliştirilmiştir (Hemaswathi vd., 2026). Önerilen sistem, yapılandırılmış veri tabanlarından bilgi çekerek öğrenci sorgularını doğal dilde yanıtlamanın yanı sıra bünyesinde barındırdığı devam hesaplayıcı gibi araçlarla üniversite personelinin idari yükünü azaltmayı hedeflemektedir. Ancak çalışmanın eğitim ortamında kullanımına ilişkin bir bilgi bulunmamaktadır.

Bu çalışmalar incelendiğinde, sistemin her derslik için sensör, kamera, RFID kart okuyucu gibi ayrı donanım gerektirmesi, geniş ölçekli kampüs uygulamalarında yüksek bir ilk kurulum maliyeti doğurmaktadır. Ayrıca öğrencilere ait parmak izi, yüz fotoğrafları gibi hassas biyometrik verilerin toplanması, KVKK, GDPR ve etik ilkeler bağlamında ciddi güvenlik ve depolama sorumlulukları getirmektedir. Diğer taraftan, incelenen bu çalışmalarda öğrencilere sorunlar büyümeden destek olma veya dijital asistanlar üzerinden rehberlik sunma gibi anlayışların geri planda kaldığı görülmektedir. Bu da mevcut sistemlerin ağırlıklı olarak denetim odaklı kalmasına neden olmaktadır. Mevcut literatür, devam kontrolünü ağırlıklı olarak idari bir veri toplama süreci olarak ele alırken, öğrencinin kampüs yaşamına katılımını tetikleyen, bağlam duyarlı rehberlik sunan ve akademik motivasyonu dinamik bildirimlerle destekleyen bir etkileşim modeli henüz tam anlamıyla olgunlaşmamış bir gelişim alanı olarak karşımıza çıkmaktadır.

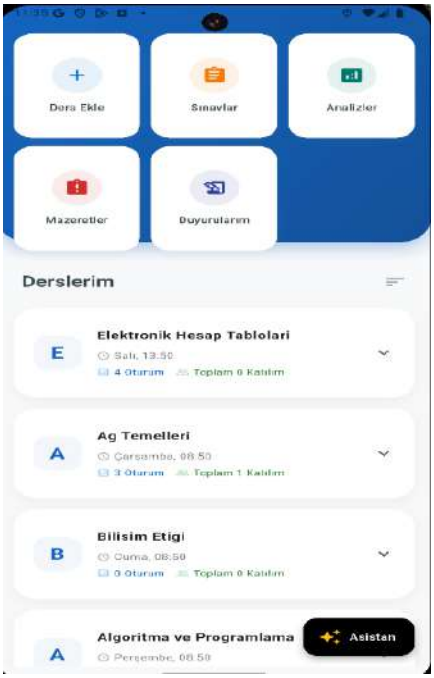
3. ÖNERİLEN SİSTEM VE METODOLOJİ

Bu çalışmada, geleneksel yoklama sistemlerinin yarattığı operasyonel zaman kayıplarını ve etik ihlalleri ortadan kaldırmak amacıyla, bulut bilişim ve yapay zekâ destekli akıllı bir öğrenci takip ve akademik asistan sistemi tasarlanmıştır. Sistem geliştirme yaşam döngüsünde (SDLC), esnekliği ve sürekli iyileştirmeyi merkeze alan "Çevik Yazılım Geliştirme" modeli benimsenmiştir. Literatürde sıklıkla karşılaşılan ve kurumlara ağır kurulum/bakım maliyetleri getiren donanım bağımlı (RFID, parmak izi, fiziksel turnike vb.) yapıların aksine, bu araştırmada tamamen yazılım tabanlı, yüksek ölçeklenebilir ve heterojen donanım altyapılarına uyumlu bir mimari kurgulanmıştır. Uygulama mimarisi Şekil 1'de sunulmuştur.



Şekil 1. Geliştirilen Uygulamanın Mimarisi.

Geliştirilen uygulama Sunum ve Etkileşim, Mantıksal Servis, Veri Katmanı olmak üzere üç modülden oluşmaktadır. Sunum ve Etkileşim Modülü öğretmen ve öğrenci rolündeki kullanıcıların sistemle temas kurduğu arayüz noktasıdır ve uygulamada arkauç tarafını ifade eder. Öğretmen ve öğrenci ana ekranına ait görseller sırasıyla Şekil 2 ve Şekil 3'te gösterilmiştir.



Şekil 2. Uygulamanın Öğretmen Ana Ekranı

Şekil 3. Uygulamanın Öğrenci Ana Ekranı

Öğretmen Arayüzünde, dersi başlatma, dinamik QR kod oluşturma görevleri bulunur. Aynı zamanda Yapay Zekâ destekli içgörüleri de bu modülde yer almaktadır. Öğrenci arayüzünde ise, QR kodu tarama ve uygulama içi bildirimleri alma işlevleri yürütülür.

Mantıksal Servis Modülü, sistemin ana omurgasını ve işleyişini oluşturur. Burada öğrenci yoklaması ile ilgili doğrulama ve güvenilirlik gibi işlemler yürütülür. Dinamik QR servisi, kodun her 60 saniyede bir değişmesini sağlayarak, sınıfta olmayan bir öğrencinin fotoğrafını paylaşarak yapılan suistimalleri minimize eder. Ayrıca ek olarak, güvenilirliği arttırmak amacıyla Geofence servisi kullanılmaktadır. Bu servis ile öğrencinin GPS konumu hesaplanır, fiziksel olarak doğru koordinatlarda yani derslik içerisinde olup olmadığını doğrular. Bu iki özelliğin yanı sıra sistemin güvenilirliğini maksimize etme amacıyla, her bir mobil cihaza sadece bir öğrenci hesabı ile giriş yapabilme kısıtı eklenmiştir. Sistemde kimlik doğrulama süreci öğretmen ve öğrencilerin akademik kayıtları üzerinden gerçekleşmektedir.

Veri Modülü**, v**erilerin güvenli bir şekilde saklandığı ve servisler arası iletişimin sağlandığı modüldür. Bulut tabanlı kimlik doğrulama sistemi kullanılarak, giriş yapan kişilerin akademik kimlikleri doğrulanır. Uygulamanın geliştirildiği Bursa Uludağ Üniversitesi örneğinde, öğrenci ve öğretmen rolleri, e-posta uzantısından anlaşılmaktadır. Yine NoSQL yapısıyla yoklama verileri, konum bilgileri ve uygulama durumlarının anlık takibi sağlanır. Ek olarak bulut tabanlı bilgilendirme sayesinde öğrencilere motivasyon mesajları veya devamsızlık uyarıları gibi anlık bildirimler gönderilir. Analiz ve Raporlama, veriyi anlamlı bilgilere dönüştüren yapay zekâ destekli bir özelliktir. Bulut sisteminde yer alan veriler kullanılarak öğrenci devamlılığı hakkında tahminleme yapılır, motivasyon içerikleri üretilir ve akademik raporlar için özetler hazırlanır. Bu modülde yer alan diğer bir yetenek, toplanan tüm dijital verinin çıktı formatına dönüştürülerek idari süreçler tamamlanır.

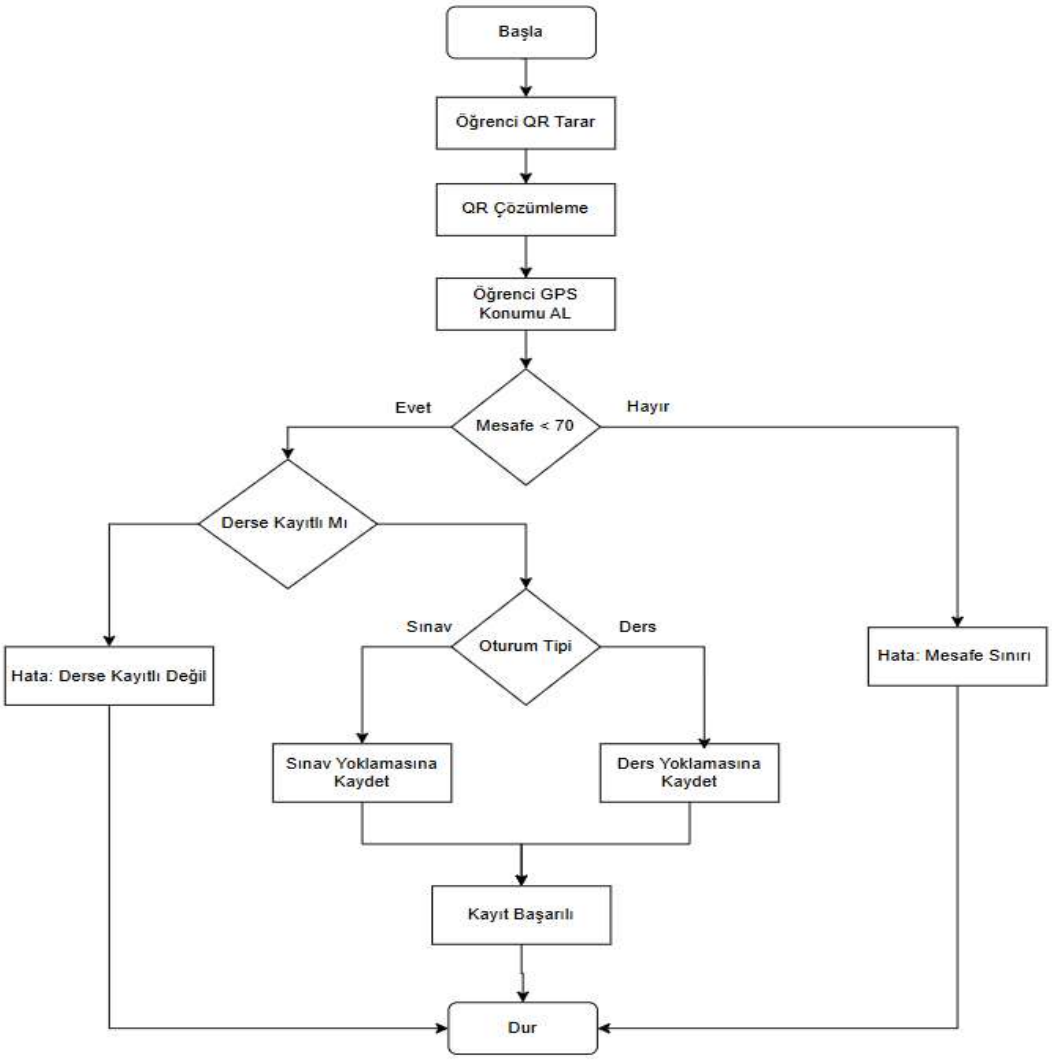
3.1. BYOD Stratejisi ve Çapraz Platform Mimarisi

Araştırmada kullanılan teknolojik altyapı, sürdürülebilirlik, maliyet-etkinlik ve maksimum erişilebilirlik prensipleri doğrultusunda BYOD stratejisi üzerine inşa edilmiştir. Sistemin uç birim yazılımları, iOS ve Android işletim sistemlerinde eşzamanlı ve yerel performans kaybı olmaksızın çalışabilmesi için çapraz platform mimarisinde geliştirilmiştir. Geliştirilen bu yazılım merkezli BYOD yaklaşımı sayesinde, eğitim kurumlarının sınıflara kurması gereken özel donanım ihtiyacı ortadan kaldırılmıştır. Bu sayede kurumsal dijital dönüşümün önündeki büyük engellerden biri olan maliyet kısıtları minimize edilmiştir.

3.2. Dinamik QR Kod ve Çok Katmanlı Konum Doğrulama Algoritması

Standart barkod veya basit e-imza tabanlı sistemlerin en büyük güvenlik zafiyeti olan, kodu kopyalayarak uzaktan yoklamaya katılma problemini azaltmak için, çalışmada Dinamik QR Kod ve Konum Tabanlı Yakınlık algoritmalarını birleşimi hibrit bir güvenlik katmanı geliştirilmiştir. Asenkron Yenilenme Algoritması, sunucu tarafında kriptografik olarak üretilen kimlik doğrulama anahtarı, istemci tarafındaki zamanlayıcı fonksiyonu aracılığıyla her 60 saniyede bir asenkron olarak güncellenmektedir. Bu kısa ömürlü yapı, üretilen kodun ekran görüntüsünün alınarak başka platformlarda paylaşılması riskini en aza indirgemektedir. Ek olarak öğretmenin hatalı derse ait QR kod üretimini önlemek amacıyla, günü ve saati gelmeyen oturumlara ilişkin QR oluşturulamamaktadır.

GPS Tabanlı Yakınlık Doğrulaması, salt optik okumayla yetinmeyerek çok katmanlı bir doğrulama mekanizmasını devreye sokar. QR kod içeriğine, oturumu başlatan öğretim elemanının cihazından alınan konum verileri gömülmüştür. Öğrenci kodu tarattığında sistem, öğrencinin anlık konum verisini çekmekte ve Haversine tabanlı matematiksel bir mesafe kıyaslaması yapmaktadır. Literatürdeki saha çalışmalarında, kapalı alanlardaki GPS sinyal sapmalarının katsayısı 0,356 olarak raporlanmıştır (Pakpahan, 2024). Uygulamanın yapıldığı ortamdaki derslikler için 50 metrelik maksimum köşegen uzunluğu varsayımı yapıldığında konumun hata eşiği yaklaşık 70 metre olarak hesaplanır. Mekânsal yakınlık eşleşmesini sağlayamayan istekler, kod doğru olsa bile güvenlik amacıyla reddedilmektedir. Sistemin bu yoklama doğrulama akış diyagramı Şekil 4'te gösterilmiştir.



Şekil 4. Yoklama Doğrulama Algoritması Akış diyagramı

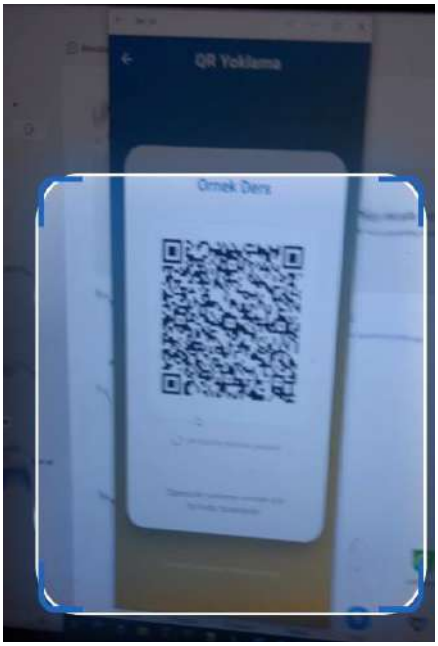
Şekil 4'te gösterilen süreç, öğrencinin öğretmenin cihazındaki dinamik QR kodu taramasıyla başlar. Uygulama, kodun içindeki şifrelenmiş veriden öğretmen GPS koordinatlarını ve oturum tipi bilgisini ayrıştırır. Geliştirilen uygulamada hem öğrencinin derse katılım durumları hem de sınava katılım bilgileri yer alabildiğinden oturum tipi ders veya sınav olabilir. Sistem, eş zamanlı olarak öğrencinin cihazından GPS verisini alır ve öğrenci ile öğretmen arasındaki mesafeyi hesaplar. Eğer mesafe hesaplanan 70 m eşik değerinden fazla ise, öğrencinin fiziksel olarak sınıfta olmadığı varsayılır ve işlem hata mesajıyla sonlandırılır.

Konum doğrulamasının geçerliliğinin ardından, sistem yoklamanın bir derse mi yoksa bir sınava mı ait olduğunu belirtir. Eğer QR kod bir sınava aitse, doğrudan sınav yoklama tablosuna kayıt yapılır. Eğer bir ders oturumu ise, ek güvenlik adımları devreye girer. Bu aşamada yetkilendirme ve token kontrolü gerçekleştirilir. Yetkilendirmede öğrencinin bu derse gerçekten kayıtlı olup olmadığı belirlenir. Token kontrolünde ise taranan QR kodun içindeki bilginin, veri tabanındaki güncel ve periyodik olarak 60

saniyede bir yenilenen token ile eşleşip eşleşmediği kontrol edilir. Tüm kontrollerden geçen işlem, veri tabanına "Başarılı" olarak kaydedilir ve öğrenciye görsel bir onay mesajı gösterilerek süreç tamamlanır.

Öğretmen ve Öğrenci için QR kod oluşturma ve okuma ekran görüntüleri sırasıyla Şekil 5 ve Şekil 6'da gösterilmiştir.

Şekil 5. Öğretmen QR Kod Oluşturma Ekranı



Şekil 6. Öğrenci QR Kod Okuma Ekranı

Bu algoritma, dinamik token kullanımı sayesinde hem ekran görüntüsü paylaşımını önler hem de GPS konum kontrolü sayesinde uzaktan yoklama verilmesini engelleyerek sistemin güvenilirliğini artırır.

3.3. Sanal Çit ile Konum Duyarlı Akıllı Bildirim Sistemi

Sistemin kullanıcı deneyimini zenginleştiren ve öğrenci devamsızlıklarını dolaylı yoldan azaltmayı hedefleyen işlevsel bileşenlerinden biri, Konum Duyarlı Akıllı Bildirim özelliğidir. Akıllı kampüs felsefesiyle uyumlu çalışan bu özellik, arka planda sanal çit algoritmasını kullanmaktadır. Sisteme önceden tanımlanmış kampüs GPS koordinatları, sanal bir sınır oluşturur. Bir öğrenci kampüs sınırlarından içeri girdiğinde, mobil cihazın konum servisleri bu durumu algılar ve sistemin akademik takvim modülünü otomatik olarak tetikler. Gerçek zamanlı saat verisi ile ders programı çapraz kontrolden geçirilir. Eğer öğrencinin başlamasına 15 dakika kalmış bir dersi bulunuyorsa sistem, cihazın ekranına doğrudan bir anlık bildirim gönderir. *"Dersinizin başlamasına 15 dakika kaldı. Ders: [Ders Adı], Konum: [Derslik/Amfi Adı]"* formatında gönderilen bu otonom bildirimler, öğrencilerin kampüs içi oryantasyonunu maksimize etmekte, zaman yönetimi konusunda bir asistanlık sunmakta ve derse geç kalma oranlarını düşürmeyi hedeflemektedir. Benzer şekilde dersi bulunan öğretmene de kampüs alanına girildiğinde uygulama içi bilgilendirme mesajı gönderilir (Şekil 7).

Şekil 7. Uygulama İçi Bildirim Mesajı Örneği

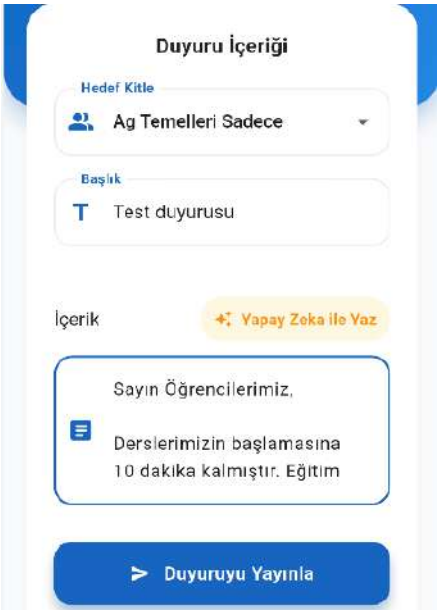
3.4. Entegre Sınav ve Oturum Yönetimi

Geliştirilen mimarinin esnekliği, sistemi sadece rutin ders yoklamalarıyla kısıtlamayıp, kurumsal akademik yönetimin en stresli süreçlerinden biri olan "Sınav Oturumu Entegrasyonu" ile ölçeklenebilir kılmıştır. Bu modül sayesinde, kâğıt tabanlı sınav giriş belgeleri tamamen dijitalleştirilmiş olup, sınav esnasındaki kimlik doğrulama ve yoklama alma süreçleri saniyeler düzeyine indirilmiştir. Ders oturumları ile sınav oturumları, arka planda farklı konfigürasyonlara sahip olmalarına rağmen aynı güvenlik mimarisi üzerinden izole bir biçimde çalıştırılmaktadır.

3.5. Üretken Yapay Zekâ Asistanı ve İzole Veri Mimarisi

Literatürdeki standart yoklama otomasyonlarından ayrılan temel husus, sisteme zeki bir karar destek mekanizması olarak Büyük Dil Modellerinin entegre edilmiş olmasıdır. Bu amaçla, güçlü doğal dil işleme yeteneklerine sahip Yapay Zeka API'si sistemin analitik motoru olarak konumlandırılmıştır. Yapay zekâ asistanı, sistemde biriken devam verilerini sürekli analiz ederek öğrencilerin devamlılık eğilimlerini saptar. Devamsızlık yasal sınırını aşma eğilimi gösteren risk grubundaki öğrencileri belirleyerek öğretim elemanlarına raporlar sunar. Yapay zekâ destekli diğer bir özellik de akademisyenlerin asgari çabayla azami verim alması için sisteme girilen birkaç anahtar kelimeden çok kısa sürede resmi, kurumsal veya daha samimi bir dil alternatifleri ile duyuru metinleri üretilebilmesidir (Şekil 8 ve Şekil 9).

Şekil 8. Anahtar kelimeden üretilmiş bir ders duyurusu



Şekil 9. AI ile üretilmiş bilgilendirme mesajı örneği

Yapay zekaya sağlanan bağlamların veri ihlali oluşturmasını engellemek için Rol Tabanlı Erişim Kontrolü seviyesi, AI sorgu katmanına kadar genişletilmiştir. Öğrenci ve eğitmen veri bağlamları sistem içinde tamamen izole edilmiş olup, yetkisiz veri çıkarımı imkânsız hale getirilmiştir.

3.6. Bilişsel Geri Bildirim

Mobil uygulama içerisine öğrencinin kendi durumunu görsel olarak algılaması ve öz-denetime katkıda bulunması amacıyla Geri Bildirim özelliği entegre edilmiştir. Bu özellikte her ders için öğrencinin katılım istatistiği gerçek zamanlı olarak sunulur (Şekil 10). Diğer taraftan öğretmen için de dersin devamına ilişkin grafiksel analizler sunularak derse katılım durumunu zamana göre analizleri sunulur (Şekil 11).

Şekil 10. Öğrenci Devam Sorgulama Ekranı

Şekil 11. Öğretmen Devam Takip Ekranı

Öğrencinin devamsızlık oranı, belirlenen yasal devamsızlık limitine yaklaştığında sistem bunu anında algılar. Renk kodlu uyarı mekanizması devreye girerek, mobil arayüzdeki grafikleri kademeli olarak dönüştürür. Bu renkli uyarılar, eşzamanlı gönderilen bildirimlerle desteklenerek dersten kalma gibi akademik başarısızlığın önüne geçmek için dijital bir akademik rehberlik hizmeti sunar.

Tasarlanan sistemin ayırt edici bir diğer özelliği, Büyük Dil Modelleri entegrasyonu sayesinde kullanıcıya veritabanı üzerinde doğal dil ile sorgulama imkânı tanımasıdır. Şekil 12'de örneklendirilen bu arayüz, öğretim elemanlarının teknik bir raporlama bilgisine ihtiyaç duymaksızın karmaşık veri setleri içerisinden anlık katılım istatistiklerini ve devamlılık paternlerini sözel komutlarla analiz etmesine olanak sağlamaktadır.

Şekil 12. Doğal Dil ile Sorgulama ve Anlamlı İçgörüler Sunma

Literatürdeki sistemlerin reaktif yapısını ve veri anlamlandırma kısıtlılıklarını aşmak amacıyla geliştirilen bu modelde LLM katmanı, erken uyarı sağlayan bir analiz mekanizması olarak konumlandırılmıştır. Sistemin sunduğu bu dinamik yetenek, yalnızca mevcut durumun raporlanmasını değil, aynı zamanda geçmiş verilerden hareketle gelecekteki katılım eğilimlerine yönelik öngörüsel çıkarımlar elde edilmesini mümkün kılmaktadır. Böylelikle önerilen ekosistem, geleneksel yöntemlerin aksine statik bir kayıt aracı olmaktan çıkarak; sınıf yönetiminde veri odaklı bir perspektif sunan, akademik başarının izlenebilirliğini artıran ve müdahale kapasitesini maksimize eden akıllı bir karar destek asistanı işlevi görmektedir.

3.7 Uygulamanın Özellikleri

Önerilen sistem, geleneksel devam kontrol mekanizmalarının ötesine geçerek kapsamlı bir 'öğrenci devamsızlık asistanı' olarak kurgulanmıştır. Bu doğrultuda sistemin fonksiyonel mimarisi sadece kayıt tutma odaklı değil, etkileşimli, proaktif ve veri analitiği temelli bir kullanıcı deneyimi sunacak şekilde tasarlanmıştır. Uygulamanın sahip olduğu temel fonksiyonlar ve bu özelliklerin operasyonel kapsamları Tablo 1'de özetlenmiştir.

Tablo 1. Geliştirilen Uygulamanın Temel Fonksiyonları

Özellik	**Açıklama**
Dinamik QR tabanlı yoklama	Statik ekran görüntüsü paylaşımını engellemek için belirli saniye aralıklarıyla yenilenen ve sunucu tarafında doğrulanan karekod mekanizması.
GPS destekli konum doğrulama	Öğrencinin yoklama işlemi sırasında sadece fiziksel olarak dersliğin koordinatları (Geofencing) içindeyse sistemin onay vermesi.
Öğrenci mazeret talebi	Sağlık raporu veya teknik aksaklık gibi durumların, öğrenci tarafından öğretim üyesinin onayına sunulması.
Sınav yoklama sistemi	Sınav yoklaması yerine geçen sınav katılım doğrulaması.
İstatistiksel analizler	Devamsızlık trendleri, ders bazlı katılım oranları ve risk grubundaki (devamsızlık sınırına yaklaşan) öğrencilerin veriye dayalı tespiti.
Anlık acil bildirimler	Derslik değişikliği, ders iptali veya kampüs içi acil durumlarda tüm öğrencilere anında ulaşan bilgilendirme mesajları.
Takvim entegrasyonu	Sistemin mobil takvim ile senkronize çalışarak, ders saatlerinin ve değişikliklerin öğrenci/hoca takviminde otomatik görünmesi.
Dijital dürtme	Devamsızlık yapan veya geç kalan öğrencilere motivasyonu artırıcı otomatik hatırlatıcılar.
BYOD	Öğrencilerin ek bir donanıma ihtiyaç duymadan kendi akıllı telefonlarını güvenli bir terminal olarak kullanabilmesi.
LLM destekli asistan	Yoklama verilerini analiz eden, "Hangi hafta katılım nasıldı?" , "ABC dersi için en riskli öğrenciler kimler?" gibi soruları yanıtlayan yapay zeka tabanlı sohbet botu.
Raporlar	Yönetimsel kararlar için Excel, PDF veya görsel grafik formatında sunulan haftalık, aylık veya dönemlik kurumsal çıktı raporları.

Tablo 1'de sunulan özellikler kümesi, önerilen sistemin literatürde sıklıkla vurgulanan operasyonel ve motivasyonel kısıtlılıklara yönelik geliştirdiği çok katmanlı yaklaşımı ortaya koymaktadır. Mevcut çözümlerin genellikle yalnızca veri toplama odaklı ve reaktif kalması, eğitim süreçlerinde bütünsel bir yönetim mekanizmasının kurulmasını zorlaştırmaktadır. Bu noktada geliştirilen model, GPS doğrulaması ve dinamik QR kod entegrasyonuyla veri bütünlüğünü güvence altına alarak geleneksel yöntemlerdeki güvenlik açıklarını minimize etmeyi hedeflemektedir.

Bunun yanı sıra, sistemin sunduğu LLM destekli asistan ve dijital dürtme mekanizmaları, veriyi sadece bir kayıt birimi olmaktan çıkarıp öğrenci bağlılığını ve öz-denetim bilincini destekleyen dinamik bir etkileşim kanalına dönüştürmektedir. Böylelikle çalışma, literatürdeki teknik güvenlik ihtiyacı ile pedagojik etkileşim eksikliği arasındaki boşluğu, düşük maliyetli ve kullanıcı merkezli bir mimariyle doldurmaya yönelik mütevazı ancak işlevsel bir çözüm önerisi sunmaktadır.

4. TARTIŞMA

Mobil yoklama sistemlerine yönelik gerçekleştirilen literatür taraması sonucunda, bu tür uygulamaların sahip olması gereken fonksiyonel ve teknik yetkinlikler, ilgili bilimsel kaynaklardaki referanslarıyla birlikte Tablo 2'de sistematik hale getirilmiştir. Tabloda, akademik çalışmalarda ön plana çıkan mobil yoklama özelliklerinin bir envanteri sunulmaktadır. Bu envanter, geliştirilen uygulamanın sunduğu çözümleri mevcut literatürle kıyaslayarak uygulamanın güçlü yönlerini ve literatüre katkı sağlayan özgün modüllerini ortaya koymak için bir temel teşkil etmektedir.

Tablo 2. Uygulamanın Sahip Olması Gereken Özellikler

No	Yetenekler	Açıklama	Kaynaklar
Y1	Mevcut Kurumsal Bilgi Sistemleri ile Entegrasyon	Sistemin öğrenci işleri veritabanı, ders programları ve kurumsal altyapılarıyla eşgüdümlü çalışması	(Çoruk vd., 2015), (Tarhan vd., 2023), (Sezdi ve Tüysüz, 2018), (Dalkılıç ve Aydın, 2018)
Y2	Ağ/Güç Kesintilerine Karşı Çevrimdışı Çalışma ve Yerel Yedekleme	İnternet veya elektrik kesintisi durumunda modülleriyle verinin korunması	(Uğuz ve Turan, 2020), (Sezdi ve Tüysüz, 2018)
Y3	Kriptografik Veri Güvenliği ve Şifreleme	Verilerin aktarımı ve depolanması sürecinde şifreleme gibi güvenlik standartların kullanılması	(Dalkılıç ve Aydın, 2018), (Sezdi ve Tüysüz, 2018), (Uçar ve Uludag, 2018)
Y4	Taşınabilirlik ve Enerji Bağımsızlığı	Harici bir elektrik şebekesine veya sabit kablo bağlantısına ihtiyaç duymaması	(Uçar ve Uludag, 2018), (Uğuz ve Turan, 2020)
Y5	Biyometrik Tanıma Teknolojileri	Kullanıcıların parmak izi veya yüz hatları üzerinden yüksek doğrulukla teşhis edilmesi	(Uğuz ve Turan, 2020), (Turan ve Doğan, 2024), (Pehlivanoğlu ve Duru, 2016)
Y6	Zorlu Koşullarda Algılama	Tıbbi maske kullanımında veya kalabalık giriş senaryolarında yüz tanıma işleminin kesintisiz sürmesi	(Turan ve Doğan, 2024)

Y7	Konum Doğrulama ve Mekânsal Yakınlık Ölçümü	Çeşitli ek teknolojiler ile öğrencinin derslikte olduğunun teyit edilmesi	(Bilen vd., 2015), (Akçay ve Altay, 2023)
Y8	Sistemi Yanıltmayı (Yerine İmza Atma) Önleyici Güvenlik Katmanları	Dinamik QR kodlar, asimetrik şifreleme ve öğretim elemanı onay mekanizmaları ile suistimallerin engellenmesi	(Dalkılıç ve Aydın, 2018), (Uğuz ve Turan, 2020)
Y9	Platform Bağımsız ve Duyarlı (Responsive) Arayüz	iOS, Android ve Web üzerinden sorunsuz erişilebilen, ergonomik ve kullanıcı dostu yazılım tasarımları	(Dalkılıç ve Aydın, 2018), (Uçar ve Uludag, 2018), (Başar ve Aslay, 2012)
Y10	İşitsel ve Görsel Geri Bildirim Mekanizmaları	Ekran uyarıları, göstergeler ve sesli uyarılar ile kişiselleştirlmiş özel bildirimlerin gönderilmesi	(Sezdi ve Tüysüz, 2018), (Turan ve Doğan, 2024)
Y11	Rol Tabanlı Erişim Kontrolü ve Yetkilendirme (RBAC)	Yönetici, akademisyen ve öğrenci yetkilerinin birbirinden izole edilerek güvenliğin artırılması	(Uçar ve Uludag, 2018)
Y12	Manuel Kayıt Düzenleme ve İstisnai Durum Yönetimi	Geç kalan veya kartını unutan öğrenciler için öğretim elemanına sunulan manuel veri girişi ve silme imkânı	(Uğuz ve Turan, 2020), (Pehlivanoğlu ve Duru, 2016)
Y13	Gelişmiş Analitik Raporlama ve İstatistik Sunumu	Öğrenci, sınıf, ders ve tarih bazlı dökümlerin otomatik raporlanması	(Sezdi ve Tüysüz, 2018), (Pehlivanoğlu ve Duru, 2016), (Yilmaz vd., 2020), (Soba, 2012)
Y14	Veri Madenciliği ve Akademik Başarı Tahminleme	Devamsızlık-başarı ilişkisinin analiz edilmesidir	(Dalkılıç ve Aydın, 2018), (Can vd., 2018)
Y15	Proaktif Bildirimler, Anlık Mesajlaşma ve Dijital Asistanlık	Coğrafi sınır tabanlı zaman duyarlı hatırlatmalar, otomatik uyarı mesajları ile akademik rehberlik sunulmasıdır	(Uçar ve Uludag, 2018), (Ertem, 2020), (Şanli vd., 2015), (Saridere ve Arslan, 2017)

Geliştirilen sistemlerin eksiklikleri, elde edilen bulgular ve önerilen yapılar incelendiğinde, başarılı ve işlevsel bir akıllı devam takip sisteminin sahip olması gereken temel kriterler Donanım ve Teknik Altyapı Kriterleri, Güvenlik ve Doğrulama Kriterleri ve Kullanıcı Deneyimi ve Operasyonel Kriterler olmak üzere üç başlık altında toplanabilir.

Donanım ve Teknik Altyapı Kriterleri: Sistem, kurumun var olan elektronik bilgi altyapısına (öğrenci işleri veritabanı, mevcut kimlik kartları vb.) entegre edilebilmeli ve devasa yeni donanım maliyetleri yaratmamalıdır. Ağ bağlantısı koptuğunda veya elektrik kesildiğinde sistemin durmaması gerekir. Verilerin cihazlar üzerinde yerel veri tabanlarında saklanması ve bağlantı sağlandığında ana sunucu ile senkronize olması verilerin kaybolmasını engeller. Bazı senaryolarda sistemin akıllı telefon, aktif internet bağlantısı veya harici bir elektrik kaynağına ihtiyaç duymadan, şarjlı ve taşınabilir bir modül şeklinde çalışabilmesi büyük esneklik sağlar.

Güvenlik ve Doğrulama Kriterleri: Verilerin yerel sunucularda veya bulutta tutulması sırasında siber güvenlik risklerine karşı gelişmiş kriptografik algoritmalar kullanılmalıdır. Öğrencilerin başkası yerine imza atmasını engellemek adına çeşitli özellikler kullanılmalı ya da süreç mutlaka bir öğretim

görevlisinin bizzat kontrolünde yürütülmelidir. Yoklamayı başlatma, sonlandırma veya cihazdaki verileri silme gibi yetkiler öğrencilere tamamen kapalı tutulmalı, sistem yalnızca öğretim görevlisinin doğrulama yapması ile bu işlemlere izin vermelidir.

Kullanıcı Deneyimi ve Operasyonel Kriterler: Hızlı, Pratik ve Temassız Kullanım: Sistem gerçek zamanlı çalışarak sınıf içi zaman kaybını minimuma indirmeli, öğrenciler açısından hijyenik ve pratik olması için tercihen temassız olmalıdır. Kullanıcıların işlemlerinin başarılı olup olmadığını anlaması için sistem, görsel veya işitsel anonslarla geri bildirim sunmalıdır. Geliştirilen yazılımların duyarlı tasarıma sahip olması gerekir, Ayrıca, sistem sadece devamsızlık saymakla kalmamalı; öğrenci bazlı, ders bazlı veya sınıf bazlı devam takiplerini detaylı istatistiklerle süzebilme imkanı vermelidir. Yine devamsızlık sınırı kritik düzeye gelen öğrencilere, sistem üzerinden otomatik uyarı gönderilerek öğrencinin mağduriyeti önceden engellenmelidir. Diğer taraftan öğrencilerin derse geç gelmesi veya gibi durumlar karşısında, sistem otomatikman bu kişileri geç kalan olarak işaretleyebilmelidir.

Tablo 2'de literatür taraması sonucunda kapsamlı bir şekilde sunulan sistem yetenekleri ve kriterleri baz alınarak, bu çalışmada geliştirilen uygulamanın mevcut durumu analiz edilmiştir. Yapılan bu nitel değerlendirme; özelliklerin karşılanma düzeyine göre 'Var', 'Yok' ve 'Kısmen' şeklinde sınıflandırılarak Tablo 3'te sunulmuştur.

Tablo 3. Geliştirilen Uygulamanın Yetenekleri

Yetenek	Yok	Var	Kısmen
Y1		✓	
Y2	✓		
Y3		✓	
Y4		✓	
Y5	✓		
Y6	✓		
Y7		✓	
Y8		✓	
Y9		✓	
Y10		✓	
Y11		✓	
Y12			✓
Y13		✓	
Y14			✓
Y15		✓	

Tablo 3 genel hatlarıyla incelendiğinde, belirlenen 15 kriterin büyük bir çoğunluğunun sistemde tam olarak karşılık bulduğu görülmektedir. Özellikle Y1, Y3, Y4, Y7, Y8, Y9, Y10, Y11, Y13 ve Y15 numaralı yeteneklerin sağlanması, sistemin fonksiyonel açıdan literatürdeki beklentileri karşılama

potansiyeli bulunduğunu göstermektedir. Tabloda görülen Y5 (Biyometrik Tanıma Teknolojileri) ve Y6 (Zorlu Koşullarda Yüz Tanıma) yeteneklerinin sistemde yer almamasının temel nedeni, KVKK ve veri güvenliği politikalarına olan tam uyum yaklaşımıdır. Biyometrik veriler, niteliği itibarıyla "özel nitelikli kişisel veri" statüsünde olup, bu verilerin işlenmesi ve saklanması ciddi hukuki sorumluluklar ve siber güvenlik riskleri barındırmaktadır. Önerilen sistem, kullanıcı mahremiyetini ve veri güvenliğini merkeze alan bir yaklaşımla, biyometrik veri toplamak yerine dinamik doğrulama yöntemlerini tercih etmiştir. Bu sayede hem etik standartlar korunmuş hem de uygulamanın yasal uyum süreçleri kolaylaştırılmıştır. Y2 kriteri olarak belirtilen çevrimdışı çalışma ve yerel yedekleme yeteneği, sistemin şu anki versiyonunda yer almamakla birlikte, sistemin sürekliliğini ve esnekliğini artırmak amacıyla bir sonraki geliştirme aşamasının temel önceliği olarak belirlenmiştir. Bu özelliğin sisteme entegrasyonu, gelecek çalışmalar kapsamında planlanmaktadır.

Y14 (Akademik Başarı Tahminleme) yeteneği için, literatürde devamsızlık verilerinin öğrenci başarısı üzerindeki etkisi bilinen bir gerçeklik olsa da bu çalışma doğrudan bir başarı analizi veya tahminleme amacı gütmemektedir. Geliştirilen sistem, veri toplama altyapısı itibarıyla bu tür bir madencilik çalışmasına potansiyel olarak imkân tanısa da mevcut aşamada bu veriler üzerinde istatistiksel bir modelleme veya korelasyon analizi gerçekleştirilmemiştir. Bu nedenle söz konusu yetenek, sistemin gelecekteki kullanım senaryolarına açık bir kapı bırakmak adına "Kısmen" olarak işaretlenmiştir. Sistem, veri suistimallerini engellemek ve kayıtların doğruluğunu garanti altına almak amacıyla geniş kapsamlı bir manuel müdahale yetkisini kısıtlamıştır. Bu nedenle Y12 sistemde sadece, mobil cihazı olmayan veya cihazını unutan öğrencilerin mağduriyetini gidermek adına, yalnızca eğitim görevlisinin sınırlı müdahalesine izin verecek şekilde tasarlanmıştır. Bu özel istisna dışında sistem tamamen otomatize doğrulama protokolleriyle çalıştığı için, genel bir manuel düzenleme imkânı sunulmamış ve bu sebeple ilgili kriter "Kısmen" olarak işaretlenmiştir.

Tablo 3'te ortaya konan karşılaştırmalı matris, sistemin mevcut haliyle literatürdeki teknik gereksinimleri karşılamadaki yetkinliğini kanıtlamakta olup; 'Kısmen' veya 'Yok' olarak işaretlenen maddeler, projenin ikinci fazı ve gelecek çalışma yol haritası için birer gelişim fırsatı olarak tanımlanmaktadır.

4.1. Pilot Uygulama Değerlendirmesi

Tasarlanan sistemin işlevselliğini ve kararlılığını test etmek amacıyla, 5 haftalık bir periyotta üç farklı akademik ders kapsamında (23, 26 ve 20 öğrenci) pilot bir çalışma yürütülmüştür. Uygulama sürecinde, yoklama işlemlerinin ortalama 5 ile 8 dakika arasında tamamlanmıştır. Bu süre geleneksel yoklama yöntemlerine kıyasla operasyonel verimlilikte önemli bir artışa işaret etmektedir.

Saha uygulaması sırasında toplam 4 öğrenci için "Mesafe sınırı aşıldı" uyarıları alınmıştır. Ancak sonraki denemelerinde öğrenciler başarılı bir şekilde sisteme giriş yapabilmişlerdir. Bu durum teknik bir arızadan ziyade mekânsal koordinatların cihazların GPS hassasiyeti gibi anlık çevresel

değişimlerinden kaynaklandığını göstermektedir. Ayrıca, fiziksel sınıf ortamında QR kodun mesafeye bağlı olarak okunabilirliği sorunu yaşanmıştır. QR kodun dijital arayüzde büyütülmesi özelliği eklenerek sorun çözülmüştür.

Mevcut çalışma, önerilen sistemin saha performansını ve operasyonel kararlılığını test etmek amacıyla yürütülen bir pilot uygulama niteliği taşımaktadır. Elde edilen bulgular, sistemin önümüzdeki akademik dönemde daha geniş öğrenci kitleleri ve farklı disiplinlerden oluşan ders kümeleriyle yaygınlaştırılmasını hedeflemektedir. Çalışmanın bir sonraki aşamasında, sistemin eğitsel deneyim üzerindeki etkilerini daha kapsamlı bir şekilde analiz edebilmek amacıyla, eğitmen ve öğrencilerin sisteme yönelik tutumlarını ölçmeye odaklanan nicel ve nitel veri toplama yöntemleri araştırma tasarımına dahil edilecektir. Bu sayede, sistemin sadece teknik işlevselliği değil, akademik süreçlerdeki kullanıcı deneyimi ve memnuniyet düzeyi de bilimsel bir temelde değerlendirilecektir.

4.2 Sistemsel Sınırlılıklar

Geliştirilen sistemin operasyonel süreçte bazı teknik sınırlılıkları bulunmaktadır. Geliştirilen uygulama, bulut tabanlı bir veritabanı mimarisi üzerinde çalışmaktadır. Bu durum İnternet bağlantısını zorunlu kılmaktadır. Ancak sistem çevrimdışı çalışma senaryolarını destekleyecek şekilde tasarlanmıştır. Cihaz arka planında veri eşitleme süreçlerini sürdürerek, bağlantının yeniden kurulduğu anda verileri güvenli bir şekilde veritabanına iletmektedir. Yine de yoklama verilerinin anlık olarak doğrulanması süreçlerinde internet bağlantısına ihtiyaç duymaktadır. Diğer bir sınırlılık sistemin konum doğrulama mekanizmasının sağlıklı çalışabilmesi için kullanıcı cihazında GPS servislerinin aktif olması zorunluluğudur. Konum servislerinin kapalı olması, sistemin güvenlik protokolü gereği katılım kaydını engellemektedir. Diğer bir sınırlılık, mevcut mobil işletim sistemlerinin sunduğu "sahte konum" (Fake GPS/GPS Spoofing) uygulamalarının, mesafe sınırlamalarını aşmaya yönelik potansiyel bir risk unsuru oluşturmasıdır. Uygulamanın bir sonraki sürümünde, bu tür girişimleri tespit edebilmek adına sadece GPS verisine değil, cihazın sunduğu diğer çevresel parametrelere (örn. baz istasyonu verisi, ağ servis sağlayıcı bilgisi vb.) dayalı çapraz doğrulama mekanizmaları üzerinde çalışılmaktadır. Gelecek geliştirme süreçlerinde, bu tür manipülasyonları engelleyecek donanım-yazılım bütünleşik doğrulama katmanlarının entegrasyonu planlanmaktadır.

5. SONUÇ VE DEĞERLENDİRME

Bu çalışma kapsamında, eğitim kurumlarındaki geleneksel devamsızlık takip süreçlerini dijitalleştirmek ve veri güvenliğini artırmak amacıyla; Dinamik QR Kod, GPS tabanlı coğrafi doğrulama, Anlık Bildirim ve LLM desteğini entegre eden yenilikçi bir mobil yoklama ekosistemi geliştirilmiştir. Literatürde yer alan 15 temel yetenek kriteri üzerinden yapılan karşılaştırmalı analizler, önerilen sistemin teknik beklentileri yüksek oranda karşıladığını ortaya koymuştur. Çalışma; sadece konum ve görsel doğrulama ile suistimallerin önüne geçmekle kalmayıp, LLM entegrasyonu sayesinde veriye dayalı akıllı geri bildirimler sunabilen, modern ve ölçeklenebilir bir mimari ortaya koymaktadır.

Çalışmanın literatüre ve uygulamaya sağladığı en temel katkı, gelişmiş teknolojik yetkinlikler ile yasal/etik uyum arasında kurduğu hassas dengedir. Literatürde yaygın olan ancak KVKK (Kişisel Verilerin Korunması Kanunu) kapsamında ciddi riskler barındıran biyometrik tanıma yöntemleri, bu çalışmada bilinçli olarak tercih edilmemiştir. Bunun yerine, dinamik QR kodların GPS verisiyle harmanlanması ve anlık bildirimlerle kullanıcı etkileşiminin güçlendirilmesi, kişisel veri güvenliğinden ödün vermeden yüksek doğruluklu bir teşhis mekanizmasının kurulabileceğini kanıtlamıştır. Ayrıca, mobil cihazı olmayan öğrenciler için eğitim görevlisine tanınan sınırlı manuel müdahale yetkisi, sistemin saha uygulamalarındaki esnekliğini ve kapsayıcılığını artırmıştır.

Gelecek perspektifinde, geliştirilen bu prototipin daha ileri seviyelere taşınması hedeflenmektedir. Mevcut versiyonda merkezi veri senkronizasyonu ve anlık bildirim akışı önceliklendirilmiş olsa da bir sonraki aşamada ağ kesintilerine karşı direnç sağlayan yerel yedekleme modüllerinin entegrasyonu planlanmaktadır. Ayrıca, sistemin halihazırda sunduğu zengin veri seti üzerinde entegre LLM desteği kullanılarak, devamsızlık örüntülerinden öğrenci başarısını tahmin eden ve akademik danışmanlık sağlayan bir karar destek mekanizmasına dönüştürülmesi projenin vizyonunu oluşturmaktadır. Bu geliştirmelerle birlikte sistemin, akıllı kampüs ekosistemlerinde sürdürülebilir ve güvenli bir dijital yönetim aracı olarak konumlanması öngörülmektedir.

KAYNAKÇA

Akçay, M., & Altay, A. (2023). İşaret yayıcı ve akıllı telefon destekli öğrenci yoklama otomasyonu. eskişehir türk dünyası uygulama ve araştırma merkezi bilişim dergisi, 4(3), 45-49. https://doi.org/10.53608/estudambilisim.1359631

Aynas, N. (2024). Birinci sınıf öğretmen adaylarının üniversiteye uyum düzeylerinin akademik öz yeterlikleri ve akademik başarılarını yordama düzeyi. İnönü Üniversitesi Eğitim Fakültesi Dergisi, 25(3), 1013-1029. https://doi.org/10.17679/inuefd.1417056

Bahşi, İ., Çetkin, M., Kervancıoğlu, P., Orhan, M., Ayan, H., Sayın, S.(2018). Tıp fakültesi derslerinin verimliliği, işleniş şekli ve öğrencilerin devam kontrolünün değerlendirilmesi. Genel Tıp Dergisi. 2018 Sep. 1;28(3):89-95.

Basit, N., Floryan, M., Hott, J. R., Huo, A., Le, J., & Zheng, I. (2025). ASCI: AI-Smart classroom initiative. Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1, 81-87. https://doi.org/10.1145/3641554.3701957

Başar, M. S., & Aslay, F. (2012). Yazılım ergonomisi: Atatürk üniversitesi öğrenci bilgi sisteminin ergonomisinin incelenmesi. Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 15(1).

Berger, R., Grané, M., Marconi, A., Fornari, F., Byxx, N., Verbraeken, V., Cole, L., Casaccio, F., Kliewe, T., Francioni, N., Mozzoni, L., & Czakert, J. P. (2025). Nudging educators toward digital innovation in higher education. 4927-4935. https://doi.org/10.21125/edulearn.2025.1250

Bilen, M., Yiğit, T., Işık, A. H. (2015). 17. Akademik bilişim konferansı - AB 2015, KNN algoritması tabanlı mobil devam takip yazılımı. ss: 256-261

Can, Ş., Özdil, T., & Yılmaz, C. (2018). Üniversite öğrencilerinin ders başarısını etkileyen faktörlerin lojistik regresyon analizi ile tahminlenmesi. International Review of Economics and Management, 6(1), 28-49. https://doi.org/10.18825/iremjournal.349984

Cankurtaran, Y. (2025). Eğitimde yenilik yönetimi ve yapay zekâ uygulamaları. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 14*(28), 119–132. https://doi.org/10.58635/ufuksbedergi.1715383

Chilakala, L. R., Ramesh, M., Fayaz, M., Bhuvanesh, K., Roy, A., & Kotla, M. (2026). Student analytics with ai-powered agent attendance System for IoT Smart Library. 2026 International Conference on Intelligent Processing, Hardware, Electronics, and Radio Systems (CIPHER), 1-5. https://doi.org/10.1109/CIPHER70417.2026.11523779

Çoruk, A., Çağatay, Ş. M., & Öztürk, H. (2015). Lisansüstü eğitimde kayıt ve devam sorunları. Sosyal Bilimler Dergisi, 2015(25).

Dalkılıç, F., & Aydın, Ö. (2018). Üniversite öğrencilerinin ders devamlarının takibine yönelik bilgi sistemi. Deu Muhendislik Fakultesi Fen ve Muhendislik, 20(60), 863-875.

Ege, F., & Özdemir, M. (2026). RFID-based non-biometric classroom attendance system: proxy attendance detection via weight sensor integration (Versiyon 1). arXiv. https://doi.org/10.48550/ARXIV.2604.22697

Ekincioğlu, P. İ., & Keser, S. (2025). Video tabanlı sınıf yoklamasının derin öğrenme ve makine öğrenmesi temelli hibrit bir yaklaşımla gerçek zamanlı olarak elde edilmesi. Sürdürülebilir Mühendislik Uygulamaları ve Teknolojik Gelişmeler Dergisi, 8(2), 163-172. https://doi.org/10.51764/smutgd.1795569

Ertem, H. Y. (2020). Üniversite birinci sınıf öğrencilerinin akademik ve sosyal uyumları: öğrenci kalıcılık programı üzerine deneysel bir çalışma. Ondokuz Mayis University Journal of Education Faculty, 39(1), 122-137.

Neelakantan, A., Satpute, P., Shinde, P., & Devang, T. M. (2025). AIOT based smart education system: a dual layer authentication and context-aware tutoring framework for learning environments (Versiyon 1). arXiv. https://doi.org/10.48550/ARXIV.2510.26999

Ömer, A. & Dalkılıç, F. (2018). Üniversite öğrencilerinin ders devamlarının takibine yönelik bilgi sistemi. DEUFMD. 1;20(60):863-75.

Özcan, C., Saray, F., & Tarı, M. (2018). Mobil cihazlar için RFID & bluetooth düşük enerji teknolojisi ile öğrenci yoklama sistemi tasarımı. *International Journal of Multidisciplinary Studies and Innovative Technologies*, *2*(1), 26-30.

Pakpahan, A. V. (2024). Convolutional neural network and haversine formula in presence system for easy attendance. 2024 Asian Conference on Communication and Networks (ASIANComNet), 1-6. https://doi.org/10.1109/ASIANComNet63184.2024.10810512

Pehlivanoğlu, M. K., & Duru, N. (2016). Üniversite öğrencilerinin devamlılığının parmak izi okuyucu cihaz kullanılarak izlenmesi. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 8(2), 9-16.

Purnamawati, P., Nuridayanti, N., Akil, M., Iskandar, A., & Pratama, M. R. (2026). Educational datafication in smart attendance systems: a bibliometric and science mapping analysis. Journal of Applied Science, Engineering, Technology, and Education, 8(1), 255–272. https://doi.org/10.35877/454RI.asci4805

Polat, E., Doğan, H. (2025). Yüz tanıma ile gerçek zamanlı öğrenci yoklama sistemi. VII. BİLSEL Uluslararası Efes Bilimsel Araştırmalar ve İnovasyon Kongresi.

S. Hemaswathi, K, T., K.B, H., R.P, S. S., & R, S. B. (2026). Next—gen university helpdesk (nexu). 2026 IEEE International Conference on Emerging Computing and Intelligent Technologies (ICoECIT), 1-6. https://doi.org/10.1109/ICoECIT68303.2026.11497274

Salunkhe, A., Pawar, V., Pise, P., Mule, S., Survase, A., Godase, V., & Zambre, S. (2025). A review on real-time RFID-based smart attendance systems for efficient record management. Advance Research in Analog and Digital Communications, 2(2), 32-46.

Sarıdere, U., & Arslan, Y. (2017). Eğitim fakültesi öğrencilerinin devamsızlık nedenleri. Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 19(2), 341-351.

Sezdi, E., & Tüysüz, B. (2018). Elektronik bilgi sistemleri tabanlı öğrenci yoklama kontrol sistemi. Bilgi Yönetimi, 1(1), 23-31. https://doi.org/10.33721/by.398269

Soba, M., (2012). Üniversite öğrencilerinin performanslarının akademisyenler tarafından analitik hiyerarşi süreci ile değerlendirilmesi: Uşak üniversitesi örneği. Elektronik Sosyal Bilimler Dergisi-Electronic Journal of Social Sciences , vol.11, no.42, 368-381.

Şanli, Ö., Altun, M., & Tan, Ç. (2015). Okula devamsızlık yapan öğrencilerin devamsızlık sebeplerinin öğrenci görüşlerine göre değerlendirilmesi. Elektronik Sosyal Bilimler Dergisi, 14(55). https://doi.org/10.17755/esosder.91015

Şılbır, G. M. (2025). Eğitimde yapay zeka ile biyometrik veri işleme: yöntemler ve uygulamalar. İçinde L. Şılbır ve D. Solak Berigel (Ed.), Eğitimde biyometrik veri: Sistemler, uygulamalar ve etik yaklaşımlar (ss. 42-57). Serüven Yayınevi.

Tarhan, S., Ünal, F., Çürükvelioğlu Köksal, E., & Büyükşahin, Y. (2023). Yükseköğretimde akademik danışmanlık: öğretim elemanlarının perspektifinden sorunlar ve çözüm önerileri. Elektronik Sosyal Bilimler Dergisi, 22(87), 776-795. https://doi.org/10.17755/esosder.1208842

Tate, A. (2023). A nudge for positive behaviours: digital nudging in higher education. Journal of Learning Development in Higher Education, (28). https://doi.org/10.47408/jldhe.vi28.1026

Turan, H., & Doğan, H. (2024). Yüz tanıma tabanlı öğrenci takip sistemi. Türk Bilim ve Mühendislik Dergisi, 6(1), 1-7. https://doi.org/10.55979/tjse.1400518

Uçar, A. & Uludağ, M. H. (2018). Nesnelerin interneti (IoT) ile akıllı sınıf ve öğrenci takip sistemi tasarımı, DÜMF MD, c. 9, sy 2, ss. 591–600, Eyl. 2018.

Uğuz, S., & Turan, Ş. (2020). Parmak izine dayalı taşınabilir özellikli öğrenci yoklama sistemi geliştirilmesi. El-Cezeri Fen ve Mühendislik Dergisi. https://doi.org/10.31202/ecjse.755754

Yilmaz, K., Şahbaz, O., Demirciler, V. O., Alıç, U., & Koca, M. (2020). Türkiye'de öğrenci devamsızlığı ile ilgili nitel bir araştırma. MANAS Sosyal Araştırmalar Dergisi, 9(3), 1440-1460. https://doi.org/10.33206/mjss.672506

Yugesh Karan,P., Sibikumar S., Haricharan U., and Sasikumar Gurumoorthy. (2024). Design and development of attendance management and analysis system using LLM. Journal of Information Technology and Digital World 6 (3): 286-301. https://doi.org/10.36548/jitdw.2024.3.007.

EXTENDED ABSTRACT

LLM-POWERED MOBİLE ATTENDANCE ASSİSTANT: A CASE STUDY OF BURSA ULUDAĞ UNİVERSİTY

Introduction and Problem Definition

The sustainability of academic success in higher education institutions is largely associated with regular student attendance. However, traditional sign-in methods or static digital solutions create operational burdens in today's crowded classroom environments and can lead to various forms of misconduct. A review of the current literature reveals that smart attendance systems often remain limited due to hardware costs, low interaction capacity, and difficulties in analyzing collected data. In particular, the high installation costs and sensitivities regarding data privacy (GDPR/KVKK) make the widespread adoption of biometric systems challenging. On the other hand, most existing systems are reactive, focusing solely on record-keeping and lacking proactive interventions to increase student motivation. This study proposes an innovative mobile ecosystem that provides both secure verification and academic guidance through Large Language Models (LLM) to address these gaps.

Methodology and System Architecture

The methodology of this study is built upon a Bring Your Own Device (BYOD) model, designed to eliminate institutional hardware dependency while ensuring high scalability and cost-efficiency. The system architecture is developed using a cross-platform framework (Flutter/Dart), enabling seamless operation across different mobile operating systems with a single codebase.

The architecture is structured into four specialized layers to ensure modularity and security:

1. **Presentation and Interaction :** The user interface is designed to provide role-specific experiences for both students and instructors. By leveraging Flutter's reactive framework, the system provides real-time updates for dynamic QR code generation and instant attendance feedback.
2. **Verification and Proximity Logic:** To prevent spoofing and ensure physical presence, the system employs a multi-layered verification framework. This includes:
    - **Dynamic QR Codes**: Generated with an asynchronous renewal algorithm that refreshes tokens every 60 seconds, rendering static screenshots useless.
    - **Proximity-Based Validation**: The system integrates GPS-based Geofencing. This ensures that attendance can only be recorded when the student is within a mathematically verified radius of the classroom.
3. **Local Intelligence and Data Management**: For high-performance data handling and offline capabilities, the architecture incorporates cloud, a lightweight and fast NoSQL database. It is utilized

to store complex objects and encrypted session tokens locally, ensuring that the application remains functional and responsive even in environments with intermittent network connectivity.

4. **LLM Integration:** The core innovation of the architecture is the integration of a Large Language Model. This layer acts as a bridge between the raw attendance data and the instructor. It processes natural language queries to identify patterns, such as at-risk students or absenteeism trends, transforming a standard database into a proactive academic assistant.

This multi-layered approach ensures that the system is not merely a digital ledger but a robust, secure, and intelligent ecosystem tailored for the modern academic environment.

Findings and Application Features

The developed application functions as a proactive academic assistant rather than a simple recording tool. Thanks to the Geofencing feature, students entering the campus boundaries are reminded of their course schedules, and academic responsibility is reinforced through "digital nudges". The most distinctive aspect of the system is the integrated LLM layer. This layer allows academics to perform complex data analysis through natural language queries such as "Which students are at the limit of absenteeism?" without the need for a technical reporting interface. Additionally, the system increases transparency by providing a self-monitoring interface where students can track their attendance status via visual charts.

Discussion and Comparison with Literature

In the analysis based on 15 fundamental capability criteria in the literature, it was observed that the proposed system provides full compliance in critical areas such as institutional integration, location verification, platform independence, and proactive notification. Biometric recognition technologies were intentionally excluded from the system to protect data privacy and ethical standards; instead, dynamic verification protocols were preferred. Compared to other existing studies, this model is evaluated as one that not only collects data but also transforms this data into educational gains by interpreting it. Features such as academic success prediction and offline operation are defined as potential areas for the system's future development phases.

Conclusion

This mobile attendance ecosystem developed for the Bursa Uludağ University case breaks the static structure of traditional methods and offers a proactive and secure management model. Academic integrity is protected through dynamic QR codes and asynchronous GPS verification, while the efficiency of administrative processes is increased with LLM support. Consequently, this study stands as a user-centered digital transformation tool with low costs, aligned with the smart campus vision. In the future, the system is aimed to be strengthened with local backup modules against network outages and to provide deeper academic counseling based on absenteeism patterns.

Cilt: 2, Sayı: 1, 2026, Sayfa: 27-45

Yönetim Bilişim Sistemleri Derneği Dergisi

ISSN: 3108-6454

Journal of Management Information Systems Association

https://www.ybs.org.tr

METİNSEL VE METADATA ÖZELLİKLERİNİ KULLANAN SAHTE İŞ İLANLARINI TESPİT ETMEYE YÖNELİK HİBRİT MAKİNE ÖĞRENMESİ ÇERÇEVESİ

Ayşe Gökçen ÇATAK [a] ve Oğuz KAYNAR [b]

Makale Bilgisi

Makale Türü
Araştırma Makalesi

Gönderim Tarihi:
16/04/2026

Kabul Tarihi:
26/06/2026

Anahtar Kelimeler:
Sahte İş İlanı Tespiti, Topluluk Öğrenmesi, XGBoost, SMOTE, Metin Madenciliği.

Özet

Çevrimiçi istihdam platformlarının hızla yaygınlaşması, sahte iş ilanlarının tespitini hem iş arayanlar hem de kurumlar açısından önemli bir sorun hâline getirmiştir. Bu çalışmada, TF-IDF tabanlı metinsel temsiller ile şirket logosu varlığı, maaş bilgisi durumu ve eksiklik sinyalleri gibi metaveri özelliklerini birleştiren hibrit bir makine öğrenmesi çerçevesi önerilmiştir. Sahte ilan oranının yalnızca %5 olduğu dengesiz veri setinde Lojistik Regresyon, Random Forest ve XGBoost modelleri; Maliyet Duyarlı Öğrenme ve SMOTE stratejileri altında karşılaştırılmıştır. Bulgular, topluluk öğrenmesi modellerinin lineer modellere göre daha başarılı olduğunu göstermiştir. Random Forest + SMOTE modeli 0.993 AUC değeriyle en yüksek performansa ulaşmıştır. Sonuçlar, hibrit özellik kullanımının yanlış pozitif oranını azaltırken yüksek duyarlılığı koruduğunu ve güvenilir tespit sağladığını ortaya koymaktadır.

[a]Yüksek Lisans Öğrenci, Sivas Cumhuriyet Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, Sivas/Türkiye, 20249348006@cumhuriyet.edu.tr , ORCID: 0009-0008-0712-853X (Sorumlu Yazar)

[b]Prof. Dr., Sivas Cumhuriyet Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, Sivas/Türkiye, okaynar@cumhuriyet.edu.tr, ORCID: 0000-0003-2387-4053 (Sorumlu Yazar)

A HYBRID MACHINE LEARNING FRAMEWORK FOR FAKE JOB POSTING DETECTION USING TEXTUAL AND METADATA FEATURES

Article Information

Article Type
Research Article

Submission Date:
16/04/2026

Acceptance Date:
26/06/2026

Keywords:
Fake Job Posting Detection, Ensemble Learning, XGBoost, SMOTE, Text Mining

Abstract

The rapid growth of online employment platforms has made fake job posting detection a critical challenge for both job seekers and organizations. This study proposes a hybrid machine learning framework that combines TF-IDF based textual representations with structural metadata features such as company logo presence, salary disclosure status, and missingness signals. Using the "Real or Fake Job Posting Prediction" dataset, where fraudulent postings constitute only 5% of all records, Logistic Regression, Random Forest, and XGBoost models were evaluated under Cost-Sensitive Learning and SMOTE strategies. Experimental findings indicate that ensemble-based models outperform linear classifiers. In particular, Random Forest combined with SMOTE achieved the highest AUC score of 0.993, demonstrating near-perfect discrimination between genuine and fraudulent postings. Results show that the hybrid feature set reduces false positive rates while preserving high recall and provides reliable detection performance for online recruitment fraud tasks.

1. GİRİŞ

Dijital iş arama platformlarının kullanımındaki hızlı artış, iş ilanlarının doğruluğunu ve güvenilirliğini kritik bir problem hâline getirmiştir. Özellikle çevrim içi platformların kolay erişilebilirliği ve denetimsiz doğası, kötü niyetli aktörlerin sahte iş ilanları oluşturarak iş arayanları dolandırmasına imkân tanımaktadır. Bu tür sahte ilanlar, kişisel bilgi hırsızlığı, haksız ücret talebi, phishing (oltalama) e-postaları ve sahte şirket profilleri gibi çeşitli güvenlik riskleri yaratmaktadır (Holt ve Bossler, 2015; Vidros vd., 2017). Europol ve ABD Federal Trade Commission (FTC) raporlarına göre, çevrim içi iş dolandırıcılığı son yıllarda önemli ölçüde artış göstermiş ve kullanıcı güvenliğini tehdit eden yaygın bir sosyal mühendislik pratiği hâline gelmiştir (Europol, 2021; FTC, 2023).

Makine öğrenmesi temelli otomatik tespit sistemleri, sahte ilanların yapısal ve dilsel farklılıklarını modelleyerek bu tür dolandırıcılık faaliyetlerinin önlenmesinde etkili bir çözüm olarak öne çıkmaktadır. Bu çalışmada, "Real or Fake Job Posting Prediction" veri seti (Vidros vd., 2017) temel alınarak metinsel ve yapısal özellikleri bütünleştiren hibrit bir sınıflandırma çerçevesi geliştirilmiştir. TF-IDF tabanlı metin temsilleri, kategorik meta-bilgiler ve eksik bilgi oranlarını (missingness patterns) içeren genişletilmiş özellik seti, tek bir boru hattı (pipeline) üzerinde birleştirilmiştir. Çalışmanın odağında, veri setindeki belirgin sınıf dengesizliği (%5 sahte ilan oranı) yer almaktadır. Bu problemi ele almak amacıyla geleneksel Lojistik Regresyon modeline ek olarak, karmaşık veri örüntülerini yakalamada başarılı olan Random Forest (Breiman, 2001) ve XGBoost (Chen ve Guestrin, 2016) algoritmaları da

araştırmaya dâhil edilmiştir. Çevrimiçi istihdam platformlarındaki sahte ilanların büyük çoğunluğu gerçek ilanlarla iç içe geçtiğinden, veri setinde ciddi bir sınıf dengesizliği ortaya çıkmaktadır. Çalışmada kullanılan veri setinde sahte ilanların oranı yalnızca %5 düzeyinde kalmaktadır; bu durum, standart eğitim yaklaşımlarıyla geliştirilen modellerin çoğunluk sınıfını (gerçek ilanları) öğrenmeye odaklanarak sahte ilanları gözden kaçırmasına zemin hazırlamaktadır. Söz konusu problemi ele almak amacıyla iki farklı yaklaşım bir arada değerlendirilmiştir. Maliyet Duyarlı Öğrenme yönteminde modelin kayıp fonksiyonuna müdahale edilerek azınlık sınıfındaki hatalara daha yüksek ceza puanı atanmış, böylece modelin sahte ilanları daha dikkatli sınıflandırması sağlanmıştır. SMOTE yönteminde ise eğitim seti içindeki dengesizlik, sentetik azınlık örnekleri üretilerek veri düzeyinde giderilmeye çalışılmıştır (Chawla vd., 2002). Her iki stratejinin lineer ve ağaç tabanlı modeller üzerindeki etkileri karşılaştırmalı biçimde analiz edilerek hangi kombinasyonun sahte ilan tespitinde daha güvenilir sonuçlar verdiği belirlenmiştir.

Bu çalışma literatüre üç temel açıdan katkı sağlamaktadır. İlk olarak, yalnızca metin içeriğine dayanmak yerine eksik veri örüntülerini ve yapısal meta-bilgileri de kapsayan hibrit bir özellik mühendisliği mimarisi geliştirilmiştir. İkinci olarak, Lojistik Regresyon, Random Forest ve XGBoost algoritmaları aynı koşullar altında sistematik biçimde karşılaştırılmış; sınıf dengesizliğini gidermek amacıyla uygulanan Maliyet Duyarlı Öğrenme ve SMOTE tekniklerinin bu modeller üzerindeki destekleyici etkileri ayrıca incelenmiştir. Üçüncü olarak, yüksek doğruluk oranı elde etmek yerine sahte ilanların gözden kaçırılma riskini en aza indirmeyi ön plana alan güvenlik odaklı bir değerlendirme çerçevesi benimsenmiş ve bu çerçevede en güvenilir model belirlenmiştir. Çalışmanın ortaya koyduğu bulgular, hem sahte iş ilanlarının yapısal ve dilsel özelliklerinin daha iyi anlaşılmasına hem de gerçek platformlara entegre edilebilecek, yüksek duyarlılıklı bir tespit sisteminin tasarımına katkı sunmaktadır.

2. KAVRAMSAL ÇERÇEVE/LİTERATÜR

Sahte iş ilanı tespiti, dijital işgücü piyasalarındaki güven sorunlarının giderek derinleşmesiyle birlikte araştırmacıların ilgisini çeken bir alan hâline gelmiştir. Literatürdeki çalışmalar, bu probleme yaklaşmak için genellikle metinsel özellikler, n-gram temsilleri veya temel meta-bilgiler üzerine kurulu sınıflandırma modelleri geliştirme yolunu tercih etmektedir.

Örneğin, Alghamdi ve Alharby (2019), SVM tabanlı özellik seçimi ile Random Forest sınıflandırıcısını birleştirerek şirket profili ve logo varlığının sahte ilan tespitinde en ayırt edici özellikler olduğunu göstermiştir. Lal vd. (2019), topluluk öğrenmesi yaklaşımının tekil sınıflandırıcılara kıyasla daha başarılı sonuçlar ürettiğini raporlamıştır. Benzer şekilde, Amaar vd. (2022), doğal dil işleme ve makine öğrenmesi tekniklerini birleştirerek sahte iş ilanlarının genellikle belirsiz dil, eksik maaş bilgisi ve aşırı cazip vaatler içerdiğini ortaya koymuştur. Kim vd. (2019) ise hiyerarşik kümeleme tabanlı derin sinir ağları aracılığıyla iş ilanı sahteciliğini tespit etmiş ve model mimarisinin sınıf dengesizliğine karşı direncinin başarımı doğrudan etkilediğini vurgulamıştır.

Metin tabanlı yaklaşımların yanında, meta-özelliklerin de sahte ilan tespitinde kritik rol oynadığı güncel çalışmalarda belirtilmiştir. Özellikle uzaktan çalışma (telecommuting) durumu, şirket logosunun yokluğu, standart dışı çalışma şekilleri ve tutarsız lokasyon bilgilerinin dolandırıcılık göstergeleri olduğu ifade edilmiştir (Mahbub vd., 2022). Ullah ve Jamjoom (2023), topluluk öğrenmesi yöntemlerini aynı veri seti üzerinde karşılaştırmalı olarak değerlendirmiş ve AdaBoost ile XGBoost modellerinin sınıf dengesizliği koşullarında güvenilir sonuçlar ürettiğini göstermiştir.

Son yıllarda derin öğrenme ve transformer tabanlı yaklaşımların sahte ilan tespitine uygulanması giderek yaygınlaşmaktadır. Akram vd. (2024), derin öğrenme yöntemlerini kullanarak çevrimiçi işe alım dolandırıcılığını tespit etmiş ve geleneksel makine öğrenmesi yöntemlerine kıyasla anlamlı performans artışları elde etmiştir. Taneja vd. (2025), BERT tabanlı Fraud-BERT modelini geliştirerek bağlam duyarlı bir tespit yaklaşımı önermiş; Varshni vd. (2025) ise transformer modellerini SHAP açıklanabilirlik yöntemiyle birleştirerek model kararlarının yorumlanabilirliğini artırmıştır. Kumar vd. (2025) ise makine öğrenmesi ve doğal dil işleme tabanlı tespit yaklaşımlarını kapsamlı biçimde derleyerek alandaki güncel eğilimleri ortaya koymuştur. Bu çalışmada transformer tabanlı modeller kullanılmamış olmakla birlikte, söz konusu yaklaşımlar gelecek araştırmalar için önemli bir yön göstermektedir. Ancak mevcut çalışmaların büyük bir bölümü ya tekil algoritmalar üzerine yoğunlaşmış ya da sınıf dengesizliğinin farklı model mimarileri üzerindeki etkisini karşılaştırmalı olarak incelemekte sınırlı kalmıştır. Bu nedenle, metinsel ve yapısal özellikleri bütünleştiren, farklı algoritmaları ve dengesiz veri stratejilerini birlikte değerlendiren hibrit yaklaşımlara ihtiyaç duyulmaktadır.

3. YÖNTEM

Bu çalışmada, çevrimiçi platformlardaki sahte iş ilanlarının yüksek doğrulukla tespiti için metinsel ve yapısal (metadata) verilerin birlikte işlendiği hibrit ve karşılaştırmalı bir makine öğrenmesi çerçevesi sunulmuştur. Çalışmanın metodolojisi, ham verinin temizlenmesinden farklı algoritmaların performans kıyaslamasına (benchmarking) kadar uzanan uçtan uca bir boru hattı (pipeline) yaklaşımını benimsemektedir (Pedregosa vd., 2011). Önerilen çerçeve dört temel aşamadan oluşmaktadır. İlk aşamada metinsel gürültüler filtrelenerek eksik veri desenleri bilgi sinyali olarak yönetilmiştir. İkinci aşamada TF-IDF tabanlı metin temsilleri ile yapısal özellikler tek bir vektör uzayında birleştirilmiştir. Üçüncü aşamada Lojistik Regresyon, Random Forest ve XGBoost algoritmaları Maliyet Duyarlı Öğrenme ve SMOTE stratejileri altında eğitilmiştir. Son aşamada ise modellerin performansı güvenlik odaklı metrikler ve ROC analizi üzerinden karşılaştırmalı olarak değerlendirilmiştir.

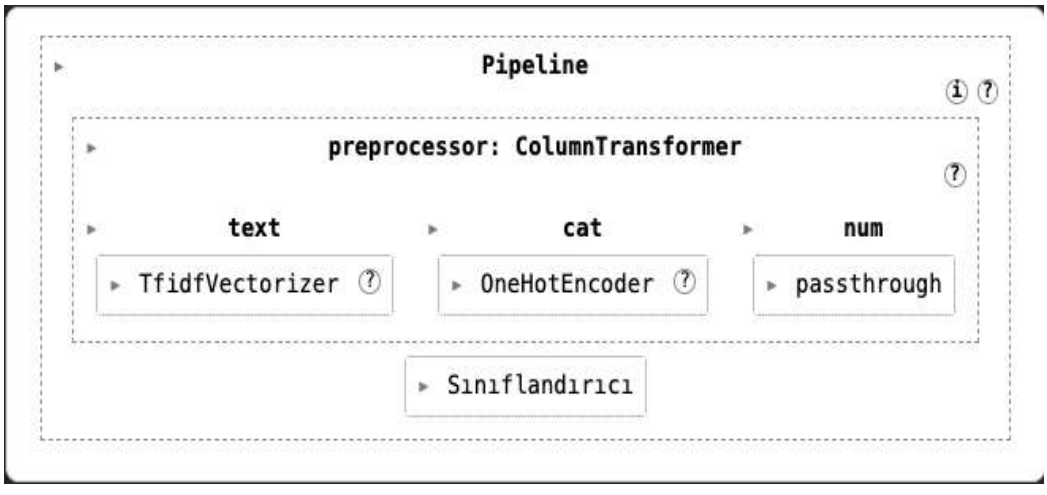
3.1. Veri Önişleme ve Özellik Yapılandırması

Analiz edilen veri seti; yapılandırılmamış metinsel içerikler, kategorik meta-bilgiler ve çeşitli eksik veri desenlerini bir arada barındıran heterojen bir yapıya sahiptir. Bu nedenle, ham veriyi analize hazırlamak için veri türüne özgü çok katmanlı bir ön işleme stratejisi izlenmiştir.

Veri temizleme aşamasında, eksik verilerin rastgele oluşmadığı, aksine sahte ilanlarda birer sinyal niteliği taşıyabileceği varsayımından hareket edilmiştir. Bu doğrultuda title, description, requirements ve company_profile gibi serbest metin alanlarındaki eksik değerler, TF-IDF vektörleştirmesinin teknik bütünlüğünü korumak amacıyla boş karakter dizisiyle doldurulmuştur. Kategorik değişkenlerdeki veri kaybı ise modelin bu durumu ayrı bir bilgi olarak öğrenmesine olanak tanımak için "Unknown" etiketiyle yeni bir sınıf olarak kodlanmıştır. Telecommuting ve has_company_logo gibi sayısal özelliklerdeki eksiklikler, yokluk durumunu temsil etmek üzere 0 değeriyle tamamlanmıştır.

Özellik mühendisliği aşamasında, veri setindeki parçalı metin alanları (başlık, açıklama, gereksinimler) tek bir text_all sütununda birleştirilerek modelin ilan içeriğini bütünsel biçimde değerlendirmesi sağlanmıştır. TfidfVectorizer aracılığıyla metinler küçük harfe dönüştürülmüş, İngilizce etkisiz kelimelerden arındırılmış ve vektör uzayına aktarılmıştır. Elde edilen metin vektörleri ile yapısal kategorik ve sayısal veriler, ColumnTransformer mimarisi aracılığıyla tek bir birleşik öznitelik uzayına dönüştürülmüştür (Pedregosa vd., 2011). Hazırlanan bu hibrit veri yapısı, çalışmada kullanılan üç farklı sınıflandırma algoritmasına (Lojistik Regresyon, Random Forest ve XGBoost) ayrı ayrı girdi olarak beslenmiştir. Şekil 1, oluşturulan pipeline mimarisini göstermektedir. Bu hibrit yapı; TF-IDF vektörlerinin sağladığı dilsel ayrım gücü ile One-Hot kodlanmış meta bilgilerin taşıdığı yapısal sinyalleri tek bir potada eriterek model başarısını artırmayı hedeflemektedir.

Şekil 1'de görüldüğü üzere, önerilen pipeline üç paralel dönüşüm kolundan oluşmaktadır. Birinci kolda (text) ham metin verisi TfidfVectorizer ile sayısal vektörlere dönüştürülmektedir. İkinci kolda (cat) employment_type, industry gibi kategorik değişkenler OneHotEncoder ile ikili vektörlere kodlanmaktadır. Üçüncü kolda (num) telecommuting, has_company_logo ve salary_provided gibi sayısal değişkenler herhangi bir dönüşüm uygulanmadan (passthrough) modele aktarılmaktadır. ColumnTransformer bu üç kolun çıktısını tek bir öznitelik vektöründe birleştirmekte, ardından bu birleşik vektör ilgili sınıflandırıcıya (Lojistik Regresyon, Random Forest veya XGBoost) girdi olarak verilmektedir.



Şekil 1. Çalışmada Kullanılan Hibrit Pipeline Mimarisi ve Sınıflandırma Süreci.

3.2. Özellik Çıkarımı

Modelin sahte ilanları yüksek başarıyla ayırt edebilmesi için, metinsel içeriklerin semantik gücü ile yapısal verilerin (metadata) ayırt ediciliğini birleştiren hibrit bir özellik seti türetilmiştir.

3.2.1. Metin Bazlı Özellikler

Birleştirilen metin verisi (text_all), sahte ilanlarda sıkça rastlanan dolandırıcılık odaklı kalıp ifadeleri (örn. "fast money", "no experience", "guaranteed income") yakalayabilmek amacıyla TF-IDF (Term Frequency-Inverse Document Frequency) yöntemiyle vektörleştirilmiştir. Vektör uzayı oluşturulurken hesaplama maliyeti ile gürültü dengesi gözetilerek korpus içerisindeki en ayırt edici 10.000 özellik seçilmiştir. Yalnızca tekil kelimeler değil kelime öbekleri de kapsanacak şekilde ngram_range=(1,2) parametresi belirlenmiş; anlamsal değeri düşük İngilizce etkisiz kelimeler (stop-words) ise vektörleştirme öncesinde listeden çıkarılmıştır.

3.2.2. Metadata ve Yapısal Özellikler

Çalışmada metinsel özelliklere ek olarak, literatürde sahtecilik sinyali taşıdığı belirtilen yapısal meta-bilgiler modele entegre edilmiştir. employment_type, required_experience, required_education, industry ve function değişkenleri, makine öğrenmesi algoritmalarının işleyebilmesi için One-Hot Encoding yöntemiyle ikili (binary) vektörlere dönüştürülmüştür. Telecommuting ve has_company_logo gibi mevcut değişkenlerin yanı sıra, ilan metinlerinin uzunluğunun dolandırıcılık tespiti için önemli bir ipucu olabileceği düşüncesiyle her bir metin alanı için kelime sayısı (word count) hesaplanarak özellik setine eklenmiştir. Bunlara ek olarak, sahte ilanlarda maaş bilgisinin genellikle gizlendiği gözleminden yola çıkılarak salary_range alanının doluluk durumuna göre salary_provided (0/1) adında ikili bir değişken türetilmiştir. Bu yaklaşım, eksik veriyi bir bilgi sinyali olarak ele alan missingness-as-information ilkesine dayanmaktadır (Little ve Rubin, 2019).

3.3. Sınıf Dengesizliği Probleminin Giderilmesi

Veri setindeki fraudulent sınıfı toplam verinin yalnızca yaklaşık %5'ini oluşturmakta olup, bu durum ciddi bir sınıf dengesizliğine (class imbalance) yol açmaktadır. Modellerin çoğunluk sınıfına (gerçek ilanlar) bias geliştirmesini önlemek ve "sahte" etiketini öğrenmelerini kolaylaştırmak için iki temel strateji karşılaştırmalı olarak uygulanmıştır:

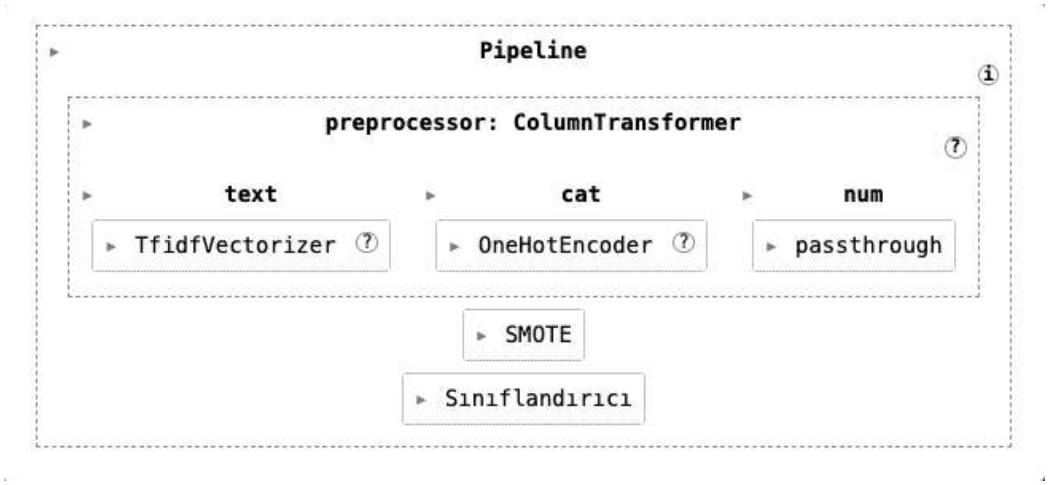
3.3.1. Maliyet Duyarlı Öğrenme (Class-Weight Adjustment)

Bu yaklaşımda, veri setini değiştirmek yerine algoritmaların maliyet fonksiyonlarına müdahale edilmiştir. Eğitim sürecinde azınlık sınıfa yapılan tahmin hatalarına daha yüksek ceza puanı atanarak modellerin duyarlılığı artırılmıştır. Bu strateji kapsamında Lojistik Regresyon ve Random Forest (Breiman, 2001) için class_weight='balanced' parametresi kullanılırken, XGBoost (Chen ve Guestrin, 2016) için eğitim setindeki pozitif ve negatif sınıf oranından hesaplanan scale_pos_weight=19.53 değeri atanmıştır.

3.3.2. Sentetik Örnekleme (SMOTE):

Eğitim setindeki dengesizliği veri düzeyinde gidermek amacıyla Synthetic Minority Oversampling Technique (SMOTE) kullanılmıştır (Chawla vd., 2002). SMOTE, azınlık sınıfına ait mevcut örneklerin k en yakın komşusu (k=5) arasında sentetik örnekler üreterek eğitim setini dengeler. Veri sızıntısını (data leakage) önlemek amacıyla SMOTE işlemi yalnızca eğitim setine uygulanacak şekilde imbalanced-learn kütüphanesinin pipeline yapısına entegre edilmiştir (Pedregosa vd., 2011). Şekil 2, SMOTE katmanının pipeline içindeki konumunu göstermektedir.

Şekil 2, SMOTE entegreli genişletilmiş pipeline mimarisini göstermektedir. Temel mimariden (Şekil 1) farklı olarak, ColumnTransformer'ın çıktısı doğrudan sınıflandırıcıya verilmemekte; araya eklenen SMOTE katmanı sentetik azınlık örnekleri üreterek eğitim setini dengelemektedir. Bu yapı sayesinde SMOTE yalnızca eğitim verisine uygulanmakta, test verisi dönüşümden etkilenmemekte ve veri sızıntısı (data leakage) riski ortadan kalkmaktadır. Dengeleme işleminin ardından elde edilen veri sınıflandırıcıya aktarılmaktadır.



Şekil 2. SMOTE Entegreli Genişletilmiş Pipeline Mimarisi.

3.4. Model Geliştirilmesi ve Algoritmik Yapı

Özellik mühendisliği aşamasında oluşturulan hibrit vektör uzayı, sınıflandırma algoritmalarına girdi olarak verilmiştir. Bu çalışmada, problemin karmaşıklığını ve dengesiz yapısını en iyi şekilde modelleyebilmek adına, farklı matematiksel temellere dayanan üç algoritma karşılaştırmalı (benchmark) olarak kullanılmıştır:

Lojistik Regresyon

Lojistik Regresyon, yüksek boyutlu ve seyrek veri yapılarında hesaplama açısından verimli sonuçlar üretmesi ve elde edilen katsayıların yorumlanabilirliği nedeniyle bu çalışmada temel referans modeli (baseline) olarak belirlenmiştir. TF-IDF tabanlı metin temsilleri doğası gereği seyrek matrisler ürettiğinden, Lojistik Regresyon bu tür verilerle teknik açıdan uyumlu bir seçimdir. Literatürde de

benzer metin sınıflandırma problemlerinde sıklıkla başlangıç noktası olarak tercih edilmekte ve daha karmaşık modellerin performansını değerlendirmek için karşılaştırma zemini oluşturmaktadır (Amaar vd., 2022).

Random Forest

Random Forest, birbirinden bağımsız karar ağaçlarının bir araya getirilmesiyle oluşturulan bir topluluk öğrenmesi yöntemidir (Breiman, 2001). Her ağacın veri setinin rastgele bir alt kümesi üzerinde eğitilmesi, modelin aşırı öğrenmeye (overfitting) karşı direncini artırmakta ve tahmin varyansını belirgin biçimde düşürmektedir. Sahte iş ilanı tespiti gibi gürültülü ve heterojen veri yapılarında bu özellik önemli bir avantaj sağlamaktadır. Alghamdi ve Alharby (2019) da aynı problemde Random Forest'ın yüksek ayırt edici güç sergilediğini göstermiştir.

XGBoost

XGBoost, gradyan artırma (gradient boosting) ilkesine dayanan ve zayıf öğrenicileri sıralı biçimde birleştirerek güçlü bir sınıflandırıcı oluşturan bir topluluk yöntemidir (Chen ve Guestrin, 2016). Metin özellikleri ile yapısal metadata arasındaki doğrusal olmayan ilişkileri modellemedeki başarısı ve sınıf dengesizliğine karşı scale_pos_weight parametresi aracılığıyla özelleştirilebilir yapısı, bu algoritmayı çalışma için uygun kılmaktadır. Ullah ve Jamjoom (2023) da aynı veri seti üzerinde XGBoost'un sınıf dengesizliği koşullarında güvenilir sonuçlar ürettiğini raporlamıştır.

Her bir algoritma için modelin başarısını ve dayanıklılığını ölçmek adına iki farklı eğitim senaryosu kurgulanmıştır. Birinci senaryoda veri setine herhangi bir müdahale yapılmadan algoritmaların kendi ağırlıklandırma parametreleri (class_weight veya scale_pos_weight) aracılığıyla azınlık sınıf hatalarına daha yüksek ceza uygulanmıştır. İkinci senaryoda ise pipeline içerisine entegre edilen SMOTE katmanı ile eğitim seti sentetik olarak dengelenerek modeller bu yeni veri dağılımı üzerinde eğitilmiştir (Chawla vd., 2002). Bu tasarım sonucunda toplamda 6 farklı deney (3 Model × 2 Senaryo) gerçekleştirilerek hangi stratejinin sahte ilan tespitinde en güvenilir sonuçları verdiği analiz edilmiştir.

3.5. Tekrar Edilebilirlik ve Hiperparametreler

Çalışmanın bağımsız olarak doğrulanabilmesi amacıyla veri bölme stratejisi, rastgelelik kontrolü ve model hiperparametreleri bu bölümde ayrıntılı biçimde açıklanmaktadır. Veri seti, sınıf oranlarını korumak amacıyla tabakalı örnekleme (stratified split) yöntemiyle %80 eğitim ve %20 test olarak ayrılmıştır. Bölme işleminde random_state=42 parametresi sabitlenmiş; SMOTE uygulamasında da aynı değer kullanılmıştır. Çalışmada tek bir sabit test seti üzerinde değerlendirme yapılmış olup çapraz doğrulama (cross-validation) uygulanmamıştır. Bu tercih, SMOTE'un yalnızca eğitim verisine uygulanması gerekliliğinden kaynaklanmakta; aksi hâlde her katlamada veri sızıntısı (data leakage) riski ortaya çıkmaktadır. Tüm modellere ait hiperparametre değerleri EK-1'de sunulmuştur.

3.6. Değerlendirme Metrikleri

Veri setindeki belirgin sınıf dengesizliği (%95 gerçek, %5 sahte ilan) göz önünde bulundurulduğunda, yalnızca doğruluk (accuracy) oranına odaklanmak yanıltıcı sonuçlar doğurabilmektedir. Zira bir model tüm ilanları "gerçek" olarak etiketlese dahi %95 doğruluk elde edebilir; oysa bu durumda sahte ilanların tamamı gözden kaçmış olur. Bu nedenle değerlendirmede güvenlik odaklı metriklere ağırlık verilmiştir.

Karışıklık matrisinden (confusion matrix) türetilen temel metrikler şu şekilde tanımlanmaktadır: Gerçekte sahte olan ve doğru tespit edilen ilanlar Doğru Pozitif (TP), gerçekte sahte olduğu halde gözden kaçan ilanlar Yanlış Negatif (FN), gerçek ilanların yanlışlıkla sahte olarak işaretlenmesi Yanlış Pozitif (FP) ve gerçek ilanların doğru sınıflandırılması Doğru Negatif (TN) olarak adlandırılmaktadır.

Bu temel değerlerden hareketle hesaplanan Recall (Duyarlılık) = TP / (TP + FN) formülüyle ifade edilmekte olup sahte ilanların ne kadarının sisteme sızdığını göstermesi bakımından güvenlik uygulamaları için en kritik metrik olarak kabul edilmektedir. Precision (Kesinlik) = TP / (TP + FP) ise sistemin meşru ilanları haksız yere engelleyip engellemediğini ölçmekte ve işveren memnuniyeti açısından önem taşımaktadır. F1-Score = 2 × (Precision × Recall) / (Precision + Recall) formülüyle hesaplanan harmonik ortalama, sınıf dengesizliği koşullarında Precision ve Recall arasındaki dengeyi tek bir değerle özetlemektedir. Son olarak ROC-AUC skoru, modelin karar eşiğinden (threshold) bağımsız olarak pozitif ve negatif sınıfları birbirinden ayırma yeteneğini karşılaştırmalı biçimde ortaya koymakta; 1'e yakın değerler neredeyse mükemmel bir ayrım gücüne işaret etmektedir.

4. BULGULAR VE TARTIŞMA

Geliştirilen hibrit tespit çerçevesinin etkinliği, ayrılan test veri seti üzerinde üç farklı algoritma (Lojistik Regresyon, Random Forest, XGBoost) kullanılarak karşılaştırmalı olarak değerlendirilmiştir. Deneysel analizler iki temel senaryo üzerine kurgulanmıştır. Birinci senaryoda veri setine herhangi bir müdahale yapılmadan algoritmalar maliyet parametreleri (Class Weight) ile eğitilmiştir. İkinci senaryoda ise eğitim aşamasında SMOTE uygulanarak sentetik veri ile dengeleme yapılmıştır. Bu bölümde her iki senaryonun model performansı üzerindeki etkileri sayısal metrikler, karışıklık matrisleri ve ROC eğrileri üzerinden detaylandırılmıştır.

4.1. Temel Modellerin Performansı

Geliştirilen hibrit çerçevenin performansı, %80 eğitim ve %20 test olarak ayrılan veri seti üzerinde altı farklı model konfigürasyonu için değerlendirilmiştir. Tablo 1, tüm modellere ait Precision, Recall, F1-Score ve AUC değerlerini karşılaştırmalı biçimde sunmaktadır.

Tablo 1. Altı Model Konfigürasyonuna Ait Karşılaştırmalı Performans Sonuçları

Model	**Precision**	**Recall**	**F1-Score**	**AUC**
Random Forest + SMOTE	1.0000	0.6994	0.8231	0.9934
Random Forest + Maliyet Duyarlı	0.9902	0.5838	0.7345	0.9914
XGBoost + Maliyet Duyarlı	0.9079	0.7977	0.8492	0.9892
XGBoost + SMOTE	0.9650	0.8671	0.8734	0.9922
Lojistik Regresyon + SMOTE	0.5869	0.8786	0.7037	0.9822
Lojistik Regresyon + Maliyet Duyarlı	0.4845	0.9017	0.6303	0.9812

Tablo 1 incelendiğinde, ağaç tabanlı topluluk modellerinin lineer modele kıyasla belirgin biçimde üstün performans sergilediği görülmektedir. En yüksek AUC değerine 0.9934 ile Random Forest + SMOTE modeli ulaşmıştır. Bu modelin Precision değerinin 1.0000 olması dikkat çekicidir; model test setinde hiçbir gerçek ilanı yanlışlıkla sahte olarak işaretlememiştir. Bununla birlikte Recall değerinin 0.6994 düzeyinde kalması, sahte ilanların yaklaşık %30'unun gözden kaçırıldığına işaret etmektedir.

Maliyet Duyarlı yaklaşımda eğitilen Random Forest modeli ise 0.9914 AUC ile ikinci sıraya yerleşmiştir. Bu modelde Recall 0.5838'e gerilemiş, ancak Precision yüksek kalmaya devam etmiştir. XGBoost + Maliyet Duyarlı ve XGBoost + SMOTE modelleri, Precision ve Recall arasında daha dengeli bir dağılım sergilemiştir. Özellikle XGBoost + SMOTE kombinasyonu 0.8671 Recall ve 0.9650 Precision değerleriyle her iki metrikte de kabul edilebilir düzeyde kalmayı başarmıştır.

Lojistik Regresyon modelleri ise her iki senaryoda da yüksek Recall sağlamasına karşın düşük Precision değerleri üretmiştir. Maliyet Duyarlı yaklaşımda Precision 0.4845'e kadar gerilemiş, bu da modelin gerçek ilanların yaklaşık yarısını yanlışlıkla sahte olarak etiketlediğine işaret etmektedir. SMOTE uygulaması Precision'ı 0.5869'a yükselterek belirli bir iyileşme sağlamış olsa da bu oran güvenlik odaklı bir sistem için hâlâ yüksek yanlış alarm riski taşımaktadır.

Confusion matrix görselleri ayrıntılı hata dağılımı açısından EK-1'de sunulmuştur.

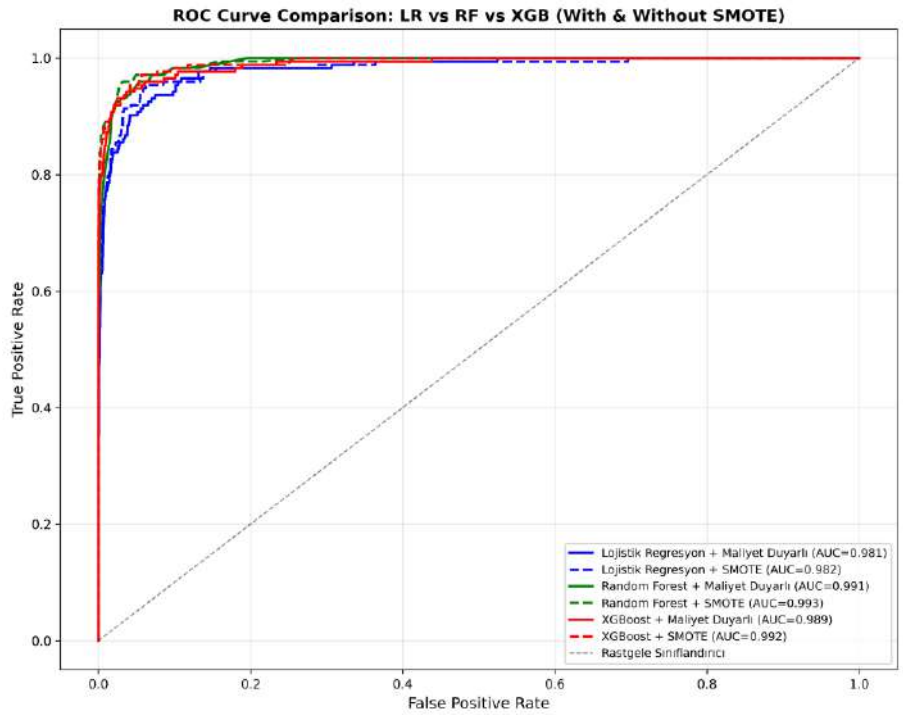
4.2. SMOTE Entegreli Modellerin Performansı

SMOTE'un model performansına etkisi algoritma mimarisine göre farklılık göstermiştir. Lojistik Regresyon modelinde etki oldukça belirgin biçimde gözlemlenmiş; Yanlış Pozitif sayısı 166'dan 107'ye gerilerken Precision değeri 0.49'dan 0.59'a yükselmiştir. Bununla birlikte bu modelin Recall değeri 0.90 düzeyinde kalmış, yüksek duyarlılık korunmuştur. Ağaç tabanlı modellerde ise SMOTE daha ölçülü ancak anlamlı katkılar sağlamıştır. Random Forest modelinde AUC 0.9914'ten 0.9934'e yükselmiş, Precision değeri 1.0000'e ulaşarak test setinde hiç yanlış alarm üretilmemiştir. XGBoost modelinde ise SMOTE ile Precision 0.9079'dan 0.9650'ye yükselmiş, Recall 0.7977 düzeyinde korunmuş; böylece yüksek kesinlik ve kabul edilebilir duyarlılık dengesi sağlanmıştır. Genel olarak SMOTE, modellerin yalnızca çoğunluk sınıfını ezberlemesini engelleyerek karar sınırlarını gerçek ve sahte ilanlar arasında daha net bir konuma taşımıştır. Confusion matrix görselleri EK-1'de sunulmuştur.

4.3. ROC Analizi ve Genel Ayrım Gücü

Geliştirilen modellerin pozitif (sahte) ve negatif (gerçek) sınıfları birbirinden ayırma yeteneği, sınıflandırma eşik değerinden bağımsız olarak ROC (Receiver Operating Characteristic) eğrileri üzerinden karşılaştırmalı olarak analiz edilmiştir. Şekil 3'te sunulan ROC eğrileri incelendiğinde, analize dahil edilen tüm modellerin uygulanan senaryodan bağımsız olarak 0.98'in üzerinde AUC skoru elde ettiği görülmektedir. Bu durum, oluşturulan hibrit öznitelik uzayının sahtecilik tespitinde güçlü bir ayrım gücü sağladığının göstergesidir.

Modeller arasında en yüksek genel ayrım gücüne 0.9934 AUC değeri ile Random Forest + SMOTE modeli ulaşmıştır. Onu 0.9914 AUC ile Maliyet Duyarlı Random Forest modeli takip etmektedir. Ağaç tabanlı modellerin (RF ve XGB) ROC eğrilerinin sol üst köşeye lineer modellere kıyasla daha dik bir açıyla yakınsadığı, yani yanlış pozitif oranını düşük tutarken yüksek duyarlılık sağladığı gözlemlenmiştir. Lojistik Regresyon modelleri ise daha geniş bir eğri çizerek daha fazla yanlış alarm üretme eğiliminde olduğunu ortaya koymuştur.



Şekil 3. Karşılaştırmalı ROC Eğrileri.

4.4. Bulguların Değerlendirilmesi / Tartışma

Elde edilen bulgular bir bütün olarak değerlendirildiğinde, önerilen hibrit mimarinin sahte iş ilanı tespitinde güçlü bir performans sergilediği görülmektedir. Literatürde genellikle göz ardı edilen missingness-as-information prensibinin bu çalışmada da geçerliliği doğrulanmıştır. Maaş bilgisinin eksikliği veya meta-verilerdeki boşluklar, metin madenciliği çıktılarıyla birleştirildiğinde modellerin

ayırt ediciliğini artırmıştır. Tüm modellerin 0.98 üzerinde AUC skoruna ulaşması, oluşturulan hibrit öznitelik setinin dilden bağımsız güçlü sinyaller taşıdığını ortaya koymaktadır.

Çalışmanın en çarpıcı bulgusu, ağaç tabanlı topluluk algoritmalarının (RF ve XGBoost) lineer modele kıyasla belirgin biçimde daha kararlı sonuçlar üretmesidir. Lojistik Regresyon yüksek Recall sağlasa da karar sınırını çizerken çok sayıda gerçek ilanı sahte olarak etiketlemiş ve düşük Precision değerleri üretmiştir. Buna karşılık Random Forest ve XGBoost, metin ve metadata arasındaki karmaşık doğrusal olmayan ilişkileri daha iyi modelleyerek yanlış alarm sayısını minimize etmiştir. Özellikle Random Forest, güvenlik sistemleri için kritik olan düşük gürültü ve yüksek tespit dengesini en iyi sağlayan algoritma olmuştur.

Sınıf dengesizliğinin giderilmesinde SMOTE tekniği model mimarisine göre farklı düzeylerde katkı sağlamıştır. Lojistik Regresyon gibi doğrusal karar sınırlarıyla çalışan modellerde bu etki oldukça belirgin biçimde gözlemlenmiş; Yanlış Pozitif sayısı 166'dan 107'ye gerilerken Precision değeri 0.49'dan 0.59'a yükselmiştir. Dengesiz bir veri setinde bu iyileşme, sistemin meşru ilanları haksız yere engellemesinin önüne geçmesi bakımından pratik önem taşımaktadır. Zaten yüksek performans sergileyen Random Forest modelinde ise SMOTE daha mütevazı ancak anlamlı bir katkı sunmuş; AUC skoru 0.9914'ten 0.9934'e yükselmiş ve modelin genelleme yeteneği pekişmiştir. Bu bulgular, SMOTE'un yalnızca azınlık sınıfını ezberletmekle kalmayıp karar sınırlarını gerçek ve sahte ilanlar arasında daha net bir konuma taşıdığına işaret etmektedir.

Elde edilen sonuçlar, alana yakın zamanda katkı sağlayan güncel çalışmalarla da karşılaştırmalı biçimde değerlendirilmiştir. Akram vd. (2024), derin öğrenme tabanlı yaklaşımlarla aynı veri seti üzerinde yüksek tespit performansı elde etmiş olmakla birlikte, bu çalışmada önerilen hibrit çerçeve geleneksel makine öğrenmesi algoritmalarıyla karşılaştırılabilir AUC değerlerine ulaşmıştır. Taneja vd. (2025) tarafından geliştirilen Fraud-BERT modeli, transformer tabanlı bağlam duyarlı bir yaklaşım sunmakta ve güçlü sınıflandırma performansı sergilemektedir; ancak bu tür modeller hesaplama maliyeti ve yorumlanabilirlik açısından ek gereksinimler doğurmaktadır. Varshni vd. (2025) ise transformer modellerini SHAP açıklanabilirlik yöntemiyle birleştirerek model kararlarının yorumlanabilirliğini artırmış; bu yaklaşım özellikle gerçek dünya uygulamalarında önemli bir avantaj sağlamaktadır. Kumar vd. (2025) tarafından gerçekleştirilen kapsamlı derleme çalışması, alandaki yöntemleri sistematik biçimde ele almakta ve makine öğrenmesi ile derin öğrenme tabanlı yaklaşımların birbirini tamamlayıcı nitelikte olduğunu ortaya koymaktadır. Bu karşılaştırma, önerilen çerçevenin hesaplama açısından verimli ve yorumlanabilir bir alternatif sunduğunu; transformer tabanlı modellerin ise özellikle yüksek kaynak ortamlarında daha ileri performans hedefleri için gelecek araştırmalara yön gösterdiğini teyit etmektedir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada, çevrim içi istihdam platformlarının güvenilirliğini tehdit eden sahte iş ilanlarının tespiti amacıyla metinsel ve yapısal öznitelikleri bütünleştiren hibrit bir makine öğrenmesi mimarisi önerilmiş ve üç farklı algoritma (Lojistik Regresyon, Random Forest, XGBoost) üzerinde kapsamlı bir kıyaslama yapılmıştır.

Gerçek dünya verileri üzerinde gerçekleştirilen deneysel analizler, salt metin madenciliği yerine eksik veri örüntülerinin (missingness patterns) ve meta-verilerin modele dahil edilmesinin ayırt edici gücü artırdığını kanıtlamıştır. Çalışmanın en çarpıcı bulgusu, ağaç tabanlı modellerin (özellikle Random Forest) lineer modellere göre sahtecilik tespitinde çok daha kararlı olduğudur. SMOTE tekniği, Lojistik Regresyon modelinde yanlış alarm sayısını 166'dan 107'ye düşürerek Precision değerini anlamlı biçimde iyileştirirken; Random Forest modelinde 0.9934 AUC skoruna ulaşılmasını sağlayarak sistemin yüksek bir ayrım gücüne sahip olduğunu doğrulamıştır.

Çalışmanın bazı sınırlılıkları da göz önünde bulundurulmalıdır. Elde edilen yüksek AUC değerleri veri setinin yapısına özgü güçlü korelasyonlardan kaynaklanıyor olabilir; bu nedenle sonuçların farklı veri setleri üzerinde doğrulanması önem taşımaktadır. Gelecek çalışmalarda metin temsili için BERT tabanlı derin dil modellerinin mimariye entegre edilmesi, transformer tabanlı yaklaşımlarla karşılaştırmalı analizlerin genişletilmesi ve sistemin dilden bağımsız (language-agnostic) yeteneklerinin geliştirilmesi hedeflenmektedir.

KAYNAKÇA

Akram, N., Irfan, R., Al-Shamayleh, A. S., Kousar, A., Qaddos, A., Imran, M., & Akhunzada, A. (2024). Online recruitment fraud (ORF) detection using deep learning approaches. *IEEE Access, 12*, 109388–109408. https://doi.org/10.1109/ACCESS.2024.3435670

Alghamdi, B. M., & Alharby, F. (2019). An intelligent model for online recruitment fraud detection. *Journal of Information Security*, *10*(3), 155–166. https://doi.org/10.4236/jis.2019.103009

Amaar, A., Aljedaani, W., Rustam, F., Ullah, S., Rupapara, V., & Ludi, S. (2022). Detection of fake job postings by utilizing machine learning and natural language processing approaches. *Neural Processing Letters*, *54*(3), 2219–2247. https://doi.org/10.1007/s11063-021-10727-z

Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research, 16*, 321–357. https://doi.org/10.1613/jair.953

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785–794). ACM. https://doi.org/10.1145/2939672.2939785

Europol. (2021). *Internet organised crime threat assessment (IOCTA) 2021*. Europol. https://www.europol.europa.eu

Federal Trade Commission (FTC). (2023). *Consumer Sentinel Network data book 2022*. Federal Trade Commission. https://www.ftc.gov

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Kim, S. H., Kim, H., & Kim, H. (2019). Fraud detection for job placement using hierarchical clusters-based deep neural networks. *Applied Intelligence, 49*(8), 2842–2858. https://doi.org/10.1007/s10489-019-01419-2

Kumar, S., Yasmeen, S., & Kumar, P. (2025). The growing threat of fake job postings: A review of machine learning and NLP-based detection approaches. *Revolutionary Advances in Computing and Electronics: An International Journal*, 41–51.

Lal, S., Jiaswal, R., Sardana, N., Verma, A., Kaur, A., & Mourya, R. (2019). ORFDetector: Ensemble learning based online recruitment fraud detection. In *Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (IC3)* (pp. 1–6). IEEE. https://doi.org/10.1109/IC3.2019.8844879

Little, R. J. A., & Rubin, D. B. (2019). *Statistical analysis with missing data* (3rd ed.). Wiley. https://doi.org/10.1002/9781119482260

Mahbub, S., Pardede, E., & Kayes, A. S. M. (2022). Online recruitment fraud detection: A study on contextual features in Australian job industries. *IEEE Access, 10*, 82776–82788. https://doi.org/10.1109/ACCESS.2022.3197225

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research, 12*, 2825–2830. https://doi.org/10.5555/1953048.2078195

Taneja, K., Vashishtha, J., & Ratnoo, S. (2025). Fraud-BERT: Transformer based context aware online recruitment fraud detection. *Discover Computing, 28*(1),9 https://doi.org/10.1007/s10791-025-09502-8

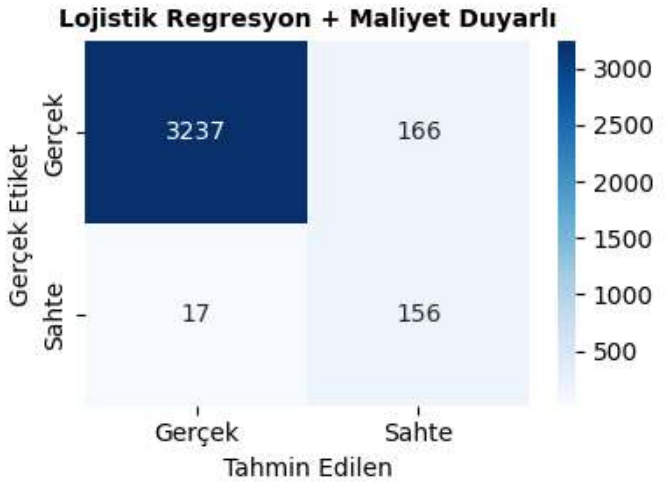
Ullah, Z., & Jamjoom, M. (2023). A smart secured framework for detecting and averting online recruitment fraud using ensemble machine learning techniques. *PeerJ Computer Science*, *9*, e1234. https://doi.org/10.7717/peerj-cs.1234

Varshni, I., Dharshini, N., & Kaviya, M. (2025). Online recruitment fraud (ORF) detection using transformer models with SHAP explainability. In *Proceedings of the IEEE International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT)* (pp. 1–8). IEEE.

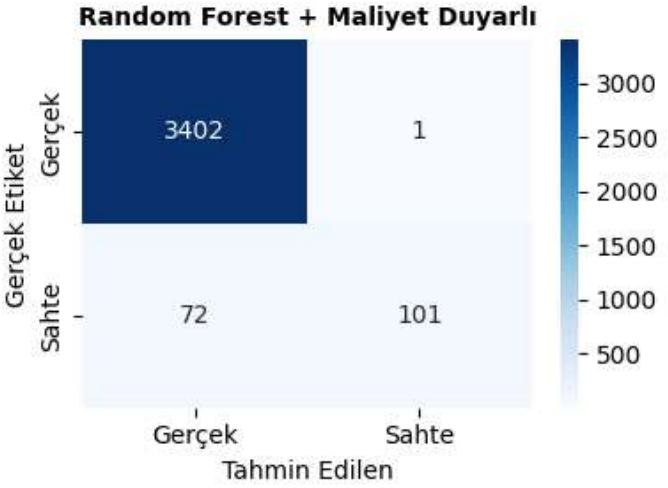
Vidros, S., Kolias, C., Kambourakis, G., & Akoglu, L. (2017). Automatic detection of online recruitment frauds: Characteristics, methods, and a public dataset. *Future Internet*, *9*(1), 6. https://doi.org/10.3390/fi9010006

EK-1. MODEL HİPERPARAMETRELERİ VE KARIŞIKLIK MATRİSLERİ

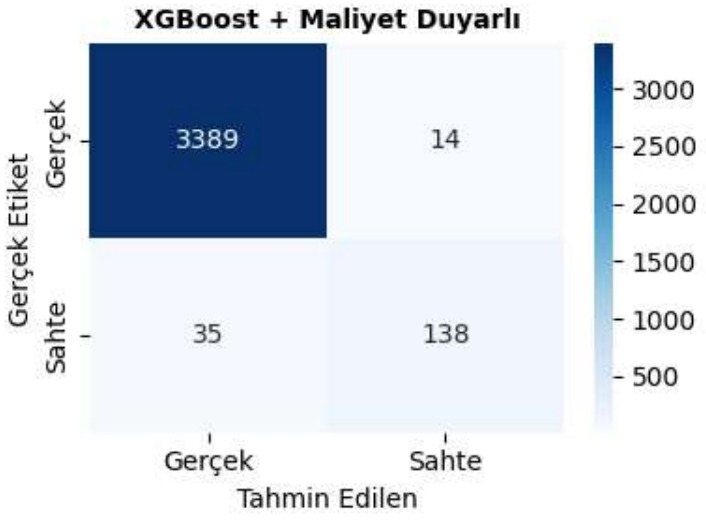
Bileşen	**Parametre**	**Değer**
Veri Bölme	test_size	0.20
Veri Bölme	random_state	42
Veri Bölme	stratify	y
TF-IDF	max_features	10.000
TF-IDF	ngram_range	(1, 2)
TF-IDF	stop_words	english
Lojistik Regresyon	class_weight	balanced
Lojistik Regresyon	max_iter	1000
Lojistik Regresyon	random_state	42
Random Forest	class_weight	balanced
Random Forest	n_estimators	100
Random Forest	random_state	42
XGBoost	scale_pos_weight	19.53
XGBoost	eval_metric	logloss
XGBoost	random_state	42
SMOTE	k_neighbors	5
SMOTE	random_state	42



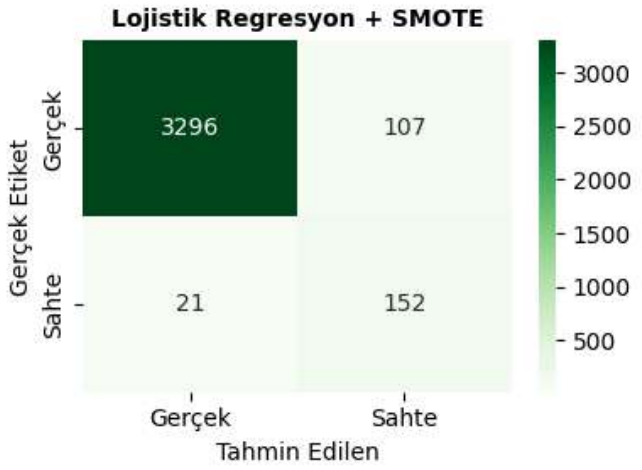
Şekil EK-1.1. Maliyet Duyarlı Lojistik Regresyon Modeline Ait Karışıklık Matrisi.



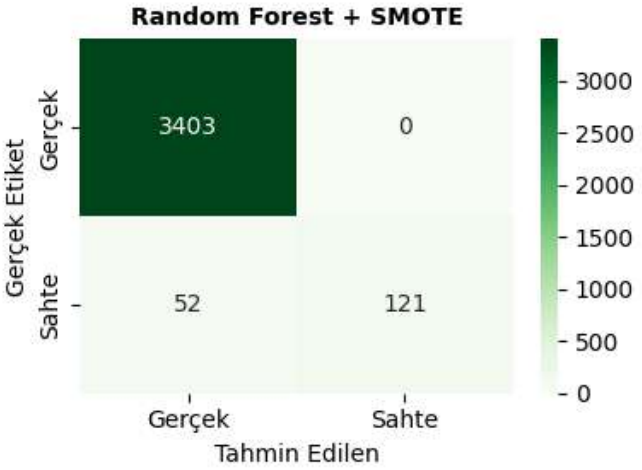
Şekil EK-1.2. Maliyet Duyarlı Random Forest Modeline Ait Karışıklık Matrisi.



Şekil EK-1.3. Maliyet Duyarlı XGBoost Modeline Ait Karışıklık Matrisi.



Şekil EK-1.4. SMOTE Destekli Lojistik Regresyon Modeline Ait Karışıklık Matrisi.



Şekil EK-1.5. SMOTE Destekli Random Forest Modeline Ait Karışıklık Matrisi.

Şekil EK-1.6. SMOTE Destekli XGBoost Modeline Ait Karışıklık Matrisi.

EXTENDED ABSTRACT

A HYBRID MACHINE LEARNING FRAMEWORK FOR FAKE JOB POSTING DETECTION USING TEXTUAL AND METADATA FEATURES

The rapid expansion of online recruitment platforms has significantly transformed hiring processes by increasing accessibility and efficiency for both employers and job seekers. However, this transformation has also created new opportunities for fraudulent actors who publish deceptive job advertisements for financial gain, identity theft, or phishing purposes. Fake job postings have become an important cybersecurity and trust issue in digital labor markets. Such advertisements often imitate legitimate recruitment announcements and may be difficult for users to distinguish manually. Therefore, developing automated and reliable detection systems has become increasingly important for protecting applicants and preserving the credibility of online employment platforms.

Previous studies on fake job posting detection have mainly focused on textual analysis, keyword extraction, linguistic patterns, or limited metadata variables. Although these approaches provide useful insights, relying only on textual content may overlook structural signals embedded in job advertisements. Features such as missing salary information, absence of company logos, incomplete firm profiles, unusual employment categories, or inconsistent metadata may also indicate suspicious activity. In this context, combining textual and structured information may improve classification performance and increase model robustness.

This study proposes a hybrid machine learning framework that integrates textual and metadata based features for fake job posting detection. The publicly available “Real or Fake Job Posting Prediction” dataset was used as the empirical basis of the study. One of the main challenges of this dataset is severe class imbalance, since fraudulent postings represent only a small proportion of the total observations. Imbalanced data structures may lead models to favor the majority class and fail to identify fraudulent cases accurately. For this reason, imbalance handling strategies were incorporated into the proposed framework.

During the preprocessing stage, textual fields such as job title, description, requirements, and company profile were combined into a single text corpus. TF-IDF vectorization was then applied to transform textual information into numerical representations. In addition, several metadata variables were included in the model, such as company logo presence, telecommuting status, salary disclosure, employment type, required experience, and education level. Missing data patterns were not ignored; instead, they were treated as potentially informative signals and converted into usable indicators.

To evaluate classification performance, three machine learning algorithms were compared: Logistic Regression, Random Forest, and XGBoost. These algorithms were selected because they represent different modeling perspectives, including linear learning and ensemble tree-based methods. Two imbalance management strategies were tested. First, cost-sensitive learning was implemented by

assigning higher penalties to minority class errors. Second, the Synthetic Minority Oversampling Technique (SMOTE) was used to generate synthetic minority class samples within the training process.

The empirical findings demonstrate that ensemble-based methods outperform the linear baseline model in terms of discrimination power and overall stability. Logistic Regression showed high sensitivity but produced relatively higher false positive rates. Random Forest and XGBoost provided more balanced results by reducing false alarms while maintaining strong recall levels. Among all tested configurations, Random Forest combined with SMOTE achieved the best overall performance with an AUC value of 0.993. This result indicates that the proposed hybrid framework can distinguish genuine and fraudulent postings with near-perfect accuracy.

The results also highlight the practical importance of metadata engineering and missingness indicators. Structural variables that may appear secondary at first glance contributed substantially to model success when combined with textual representations. This suggests that fraud detection systems should not rely exclusively on language patterns but instead adopt multidimensional feature architectures.

From a managerial perspective, the proposed model can be integrated into online recruitment platforms as an early warning or decision support system. Suspicious advertisements can be flagged automatically before publication or routed to human moderators for further review. Such applications may reduce reputational risks for platforms and protect job seekers from potential scams.

In conclusion, this study shows that hybrid machine learning architectures offer a highly effective solution for fake job posting detection under imbalanced data conditions. Future studies may extend this framework by incorporating transformer-based language models such as BERT, multilingual datasets, and real-time streaming environments.

Cilt: 2, Sayı: 1, 2026, Sayfa: 46-64

Yönetim Bilişim Sistemleri Derneği Dergisi

ISSN: 3108-6454

Journal of Management Information Systems Association

https://www.ybs.org.tr

DENİZCİLİK SİBER GÜVENLİĞİNDE PROAKTİF BİR SAVUNMA YAKLAŞIMI: HÜRMÜZ BOĞAZI LİMANLARININ OSINT TABANLI AMPİRİK HARİTALAMASI

Aleyna YILDIZ[a] ve Hüseyin PARMAKSIZ[b]

Makale Bilgisi

Makale Türü
Araştırma Makalesi

Gönderim Tarihi:
19/05/2026

Kabul Tarihi:
26/06/2026

Anahtar Kelimeler:
Siber Güvenlik, OSINT, Liman 4.0, Sosyal Mühendislik, Millileşme.

Özet

Denizcilik sektöründeki dijitalleşme, küresel tedarik zincirlerini asimetrik siber tehditlere açık hale getirmektedir. Bu araştırma, Hürmüz Boğazı'ndaki on stratejik otoritenin siber güvenlik altyapılarını Açık Kaynak İstihbaratı (OSINT) kullanarak ampirik olarak incelemektedir. Hedef sistemlerin dijital ayak izleri Python tabanlı otomasyonla haritalandırılmış; tehdit söylemleri ise 106 güncel haber kaynağı üzerinden Doğal Dil İşleme ile analiz edilmiştir. Bulgular, Körfez ülkelerinde veri egemenliği ile bulut bağımlılığı arasında ikilem yaşandığını ve İran'ın agresif Web Uygulama Güvenlik Duvarı konfigürasyonlarıyla devlet destekli siber izolasyon stratejisi izlediğini göstermektedir. Ayrıca Liman 4.0 ekosisteminde en zayıf halkanın insan faktörü olduğu tespit edilmiş; sosyal mühendislik riskleri ile donanımda millileşme ihtiyacı vurgulanmıştır. Metin madenciliği sonuçları, siber tehdit algısının basit veri hırsızlığından ziyade fiziksel operasyonel teknoloji unsurlarıyla doğrudan bağlantılı olduğunu doğrulamaktadır. Son olarak, denizaltı fiber optik kablolarının stratejik önemine dikkat çekilerek NIS2 gibi proaktif mevzuatların ulusal denizcilik stratejilerine entegre edilmesi önerilmektedir.

[a] Lisans Öğrencisi, Bilecik Şeyh Edebali Üniversitesi, Yönetim Bilişim Sistemleri, Bilecik/Türkiye, 5933986@ogrenci.bilecik.edu.tr, ORCID: 0009-0006-9724-1442 (Corresponding Author)
[b] Dr. Öğr. Üyesi, Bilecik Şeyh Edebali Üniversitesi, Yönetim Bilişim Sistemleri, Bilecik/Türkiye, huseyin.parmaksiz@bilecik.edu.tr, ORCID: 0000-0001-8455-5625

A PROACTIVE DEFENSE APPROACH IN MARITIME CYBERSECURITY: AN OSINT-BASED EMPIRICAL MAPPING OF STRAIT OF HORMUZ PORTS

Article Information

Article Type
Research Article

Submission Date:
19/05/2026

Acceptance Date:
26/06/2026

Keywords:
Cybersecurity, OSINT, Port 4.0, Social Engineering, Nationalization.

Abstract

Digitalization in the maritime sector exposes global supply chains to asymmetric cyber threats. This research empirically examines the cybersecurity infrastructures of ten strategic authorities in the Strait of Hormuz using Open-Source Intelligence (OSINT). Target systems' digital footprints were mapped via Python-based automation, while threat discourses from 106 news sources were analyzed using Natural Language Processing. Findings reveal a dilemma between data sovereignty and cloud dependency in Gulf states, alongside Iran's state-sponsored cyber isolation strategy driven by aggressive Web Application Firewall configurations. Additionally, the human factor emerged as the weakest link in the Port 4.0 ecosystem, emphasizing social engineering risks and the need for hardware nationalization. Text mining confirms that cyber threat perceptions are directly linked to physical operational technologies rather than simple data theft. Finally, stressing the strategic importance of submarine cables, this study recommends integrating proactive legislations like the NIS2 Directive into national maritime strategies.

1. GİRİŞ

Denizcilik sektörü, küresel ticaretin bel kemiğini oluşturmanın ötesinde, ülkelerin ekonomik refahı ve ulusal güvenliği için stratejik bir yaşam hattı niteliğindedir. Dünya ticaret hacminin yaklaşık %80'inin deniz yolları üzerinden gerçekleşmesi (UNCTAD, 2023), bu sektörü dijitalleşen dünyada kritik bir hedef hâline getirmiştir. Özellikle "Liman 4.0" ve otonom gemi mimarileri (De la Peña Zarzuelo vd., 2020) gibi devrim niteliğindeki gelişmelerle birlikte denizcilik operasyonları, geleneksel fiziksel sınırların ötesine geçerek siber-fiziksel sistemlerin iç içe geçtiği karmaşık bir dijital ekosisteme dönüşmüştür. Ancak bu teknolojik sıçrama, yönetilmesi güç bir saldırı yüzeyini de beraberinde getirmiştir. Nesnelerin İnterneti (IoT) kapsamında yer alan akıllı vinçler, bulut tabanlı Otomatik Tanımlama Sistemi (AIS) cihazları ve Radyo Frekansı ile Tanımlama (RFID) tabanlı konteyner takip sistemlerinden otonom seyrüsefer altyapılarına kadar her yeni bağlantı, küresel tedarik zinciri açısından potansiyel bir siber zafiyet kapısı aralamaktadır.

Bu siber-fiziksel risklerin en somut ve en kritik hissedildiği stratejik düğüm noktalarının (Süveyş Kanalı, Malakka Boğazı ve Panama Kanalı gibi) başında Hürmüz Boğazı gelmektedir. Jeopolitik önemi nedeniyle dünya enerji trafiğinin en hassas noktası kabul edilen bu bölge, konvansiyonel askeri tehditlerin yanı sıra sofistike siber operasyonların da odak noktasındadır. Bölgedeki liman otoritelerine yönelik olası bir siber müdahale, yalnızca bölgesel bir aksaklığa değil; tedarik zinciri felç olacağı için küresel ölçekte bir enerji krizine ve ekonomik dalgalanmaya (Clavijo Mesa vd., 2024) yol açma

potansiyeli taşımaktadır. Dolayısıyla bu bölgedeki stratejik aktörlerin siber güvenlik duruşlarını anlamak, küresel güvenlik için bir zorunluluk haline gelmiştir.

Denizcilik siber güvenliği üzerine yapılan çalışmaların büyük bir kısmının teorik çerçeveler, genel risk modelleri veya yaşanmış veri ihlallerinin geriye dönük incelemeleri etrafında toplandığı görülmektedir (Kavallieratos ve Katsikas, 2020; Svilicic vd., 2019). Araştırmacıların birçoğu laboratuvar ortamındaki simülasyonlara veya anket verilerine dayanarak siber riskleri tanımlamaya çalışmıştır. Örneğin, Hemminghaus vd. (2021) kapalı bir ağ içi tehdit modellemesi geliştirmiş olsa da bu tür yaklaşımlar, gerçek dünyadaki dinamik ve karmaşık saldırı yüzeylerini yansıtmakta eksik kalmaktadır. Siber tehditlerin saniyeler içinde değiştiği günümüzde, stratejik kurumların dışa açık ağ altyapılarını gerçek zamanlı ve nesnel yöntemlerle haritalandıran deneysel (ampirik) çalışmaların eksikliği dikkat çekmektedir.

Bu çalışma, literatürdeki söz konusu boşluğu doldurmak amacıyla tasarlanmış olup teorik varsayımların ötesine geçerek doğrudan OSINT verilerine odaklanmaktadır. Araştırma kapsamında, bölgenin siber ekosistemini şekillendiren on stratejik denizcilik otoritesi, Patton (2015) tarafından çerçevesi çizilen "Amaçlı Örnekleme" yöntemiyle belirlenmiş ve bu kurumların dijital ayak izleri analiz edilmiştir. Çalışmanın temel motivasyonu; bu kurumların siber güvenlik stratejilerini veri egemenliği, uluslararası bulut bağımlılığı ve proaktif savunma mekanizmaları bağlamında yapısal olarak ortaya koymaktır.

2. KAVRAMSAL ÇERÇEVE/LİTERATÜR

Denizcilik siber güvenliği literatürü incelendiğinde, çalışmaların son beş yılda teorik risk analizlerinden ampirik teknik analizlere doğru evrildiği gözlemlenmektedir. Literatürdeki araştırmalar genel olarak gemi içi sistemlerin güvenliği (Svilicic vd., 2019), liman altyapılarının dayanıklılığı (De la Peña Zarzuelo vd., 2020) ve OSINT tabanlı tehdit istihbaratı (Nasr vd., 2026) olmak üzere üç ana eksende toplanmaktadır. Mevcut çalışmaların büyük bir kısmı anket ve simülasyon temelli olup, Hürmüz Boğazı gibi jeopolitik açıdan kritik bölgelerin gerçek zamanlı dijital ayak izlerini inceleyen ampirik OSINT araştırmalarının literatürde son derece kısıtlı olduğu tespit edilmiştir. Bu durumun temel nedeni; ulusal güvenlik kapsamında agresif güvenlik duvarlarıyla (WAF) korunan liman altyapılarından gerçek zamanlı dijital veri toplamanın barındırdığı yasal ve etik zorluklar ile araştırmacıların genellikle kontrollü kapalı devre simülasyon (testbed) ortamlarını tercih etmesidir. Bu çalışma, Tablo 1'de sunulan 30 referans makalenin işaret ettiği söz konusu metodolojik ve coğrafi boşluklardan yola çıkarak kurgulanmıştır.

Tablo 1. Denizcilik Siber Güvenliği Literatür Özeti

Çalışma	**Odak Konusu**	**Kullanılan Yöntem / Araç**	**Temel Bulgu**
Puchkov vd. (2021)	Siber Olay Tespiti	Büyük Veri, SpaCy tabanlı Doğal Dil İşleme (NLP) ve Metin Madenciliği	İnternet tabanlı metinlerden otomatik siber tehdit bilgisi çıkarılabileceği kanıtlanmıştır.
Hemminghaus vd. (2021)	Köprü Sistemi Güvenliği	Köprü Siber Güvenlik Aracı (BRAT) Destekli İnteraktif Saldırı Simülasyonu	Tasarım aşamasında zafiyet tespiti sağlayan bir simülasyon aracı geliştirilmiştir.
Androjna vd. (2021)	Sinyal Manipülasyonu	Küresel Navigasyon Uydu Sistemleri (GNSS) ve AIS SWOT Analizi	Navigasyon sistemlerinin şifreleme eksikliği nedeniyle spoofing'e çok açık olduğu saptanmıştır.
Jacq vd. (2021)	Kriz Yönetimi Eğitimi	Hibrit Siber Poligon (Cyber Range)	Liman aktörlerinin siber eğitiminde poligon kullanımının etkili olduğu görülmüştür.
Tam vd. (2021)	Siber-Fiziksel Güvenlik	Donanım Test Yatağı (Testbed)	Saldırıların fiziksel güvenlik üzerindeki etkileri ve gemi-liman riskleri somutlaştırılmıştır.
Nissov vd. (2021)	Siber Dayanıklılık	Topolojik Bilgi Akışı Analizi	Saldırı kaynaklı hatalı verilerin tespit edilip izole edilebileceği modellenmiştir.
He vd. (2021)	Ağ İçi Tehdit Modellemesi	Markov Zinciri ve Alan Adı Sistemi (DNS) Rebinding	IoT cihazlarını korumak adına DNS saldırılarını başlatan etkili bir tespit mekanizması sunulmuştur.
(Okolo ve Chang, 2021)	Tedarik Zinciri Direnci	Sistematik Derleme ve Yapay Zeka	Denizcilik ağlarında yapay zeka destekli anomali tespitinin kritik olduğu gösterilmiştir.
Gunes vd. (2021)	Liman Risk Değerlendirmesi	Senaryo Tabanlı Risk Analizi	Limanların siber ve fiziksel altyapılarının entegre değerlendirilmesinin zorunluluğu kanıtlanmıştır.
Rajaram ve Benson, (2022)	Siber Risk Yönetimi	OT Sistemleri Analizi	Donatanlar için siber hijyeni artıracak detaylı bir kontrol listesi geliştirilmiştir.
Oruc vd. (2022)	Entegre Navigasyon Sistemi (INS)	MITRE ATT&CK Çerçevesi	Navigasyon sistemlerinde potansiyel siber riskler tanımlanmış ve sınıflandırılmıştır.
Schwarz ve von Solms, (2022)	Bilgi Güvenliği Vakaları	Yapılandırılmış Uzman Mülakatı	Tehditlerin küçümsendiği ve sektörde bilgi paylaşımı platformları kurulması gerektiği vurgulanmıştır.
Gyamfi vd. (2022)	IoT Ağ Güvenliği	Uyarlanabilir Artımlı Pasif-Agresif Makine Öğrenmesi (AI-PAML)	Uç Bilişim (MEC) ile IoT cihazlarında yüksek doğrulukla saldırı tespiti yapılmıştır.
Grispos ve Mahoney (2022)	Sektörel Meydan Okumalar	Tarihsel Vaka Analizi	Teknolojinin benimsenme hızının güvenliği geçtiği ve finansal açıklar doğurduğu bulunmuştur.

Amro vd. (2022)	Otonom Gemi Güvenliği	Hata Türü, Etkileri ve Kritiklik Analizi (FMECA) ve MITRE ATT&CK	Otomasyon ve uzaktan bağlantıların riskleri artırdığı ve tehdit tabanlı savunma gerektiği belirlenmiştir.
Farah vd. (2022)	IoT ve Büyük Veri Etkisi	Sistematik Literatür Taraması	Akıllı sistemlerin GNSS gibi altyapılardaki siber saldırı oranını devasa ölçüde artırdığı saptanmıştır.
Yadav ve Kumar (2023)	Açık Kaynak İstihbaratı	Makine Öğrenmesi Derlemesi	OSINT'in yapay zeka ile otonomlaştırılmasının ulusal güvenlikteki önemi tartışılmıştır.
Pöyhönen ve Lehto (2023)	Kapsamlı Liman Güvenliği	Sistemler Sistemi Yaklaşımı	Siber güvenliğin teknik bir sorundan ziyade bütüncül bir yönetim süreci olması gerektiği saptanmıştır.
Lee ve Lee (2023)	Gemi Veri Sunucuları	Mesaj Kuyruklama Telemetri Aktarımı (MQTT) Protokolü Modifikasyonu	Önerilen yöntemin veri sunucularını DDoS saldırılarına karşı daha dayanıklı hale getirdiği kanıtlanmıştır.
Progoulakis ve Nikitakos, (2023)	Siber-Fiziksel Dijitalleşme	Bow Tie Analizi ve Amerikan Petrol Enstitüsü Güvenlik Risk Değerlendirmesi (API SRA)	Liman altyapılarındaki risklerin proaktif ve reaktif yöntemlerle yönetilebileceği gösterilmiştir.
Jouni Pöyhönen (2023)	Akıllı Terminal Süreçleri	Bütüncül Araştırma Yaklaşımı	Liman bilişim sistemlerinin enerji ve bilgi akışıyla birlikte holistik değerlendirilmesi gerektiği saptanmıştır.
Rebecca Rohan (2023)	Siber Saldırı Trendleri	Elmas Modeli (Diamond Model)	Nakliye şirketlerinin veri sızdırma amacıyla devlet destekli aktörlerce yoğun hedef alındığı bulunmuştur.
Pijpker ve McCombie (2023)	Tehdit İstihbaratı (CTI)	Gemi Honeynet (Tuzak Ağ) Tasarımı	Yaşlanan sistemlere saldıran aktörleri gözlemlemek için tuzak ağların etkili olduğu vurgulanmıştır.
Amro ve Gkioulos (2023)	Tehdit Bilgili Savunma	Sistem Yaşam Döngüsü Analizi	Otonom gemi sistem döngüsünün aşamalarında zafiyet değerlendirmesinin iyileştirilebileceği saptanmıştır.
Shi ve Zhang (2023)	Siber Tehdit Farkındalığı	Siber Tehdit Uzamsal-Zamansal Dönüştürücü (ActSTT) Derin Öğrenme Modeli	Gelişmiş kalıcı tehditlerin (APT) tanımlanmasında %98'in üzerinde yüksek doğruluk elde edilmiştir.
Pijpker ve McCombie (2024)	Denizcilik Saldırı Veritabanı	Veritabanı (MCAD) Analizi	290'dan fazla siber olayın analiziyle tehdit aktörü profilleri ve saldırı sıklığı ortaya konmuştur.
Hacks ve Pahl (2024)	Liman Çağrı Operasyonları	Meta Saldırı Dili (MAL) Tabanlı harborLang ve Siber Risk Değerlendirme Çerçevesi (YACRAF)	Liman operasyonlarında detaylı saldırı simülasyonlarıyla güvenlik duruşunun artırılabileceği gösterilmiştir.

Mesa vd. (2024)	Siber Saldırı Taksonomisi	Sistematik Derlemeler ve Meta-Analizler İçin Tercih Edilen Bildirim Öğeleri (PRISMA) Yöntemi	Endüstri 4.0 tabanlı lojistik zincirinde en büyük tehditlerin DDoS ve fidye yazılımlar olduğu bulunmuştur.
Keskin vd. (2025)	Sistematik Tehdit Modellemesi	Saldırı Ağaçları (Uzman Mülakatı)	Rotadan çıkarma veya iletişimi kesme senaryolarının gerçekçi kurgulanabileceği kanıtlanmıştır.
Nasr vd. (2026)	Proaktif Siber Savunma	OSINT Çerçevesi	OSINT'in denizcilik bağlamında siber saldırıları önlemedeki kritik rolü akademik düzeyde tartışılmıştır.

Literatürdeki Boşluk ve Çalışmamızın Özgün Değeri

Tablo 1'de özetlenen güncel denizcilik siber güvenliği literatürü incelendiğinde, araştırmaların önemli bir kısmının simülasyon araçlarına (Hemminghaus vd., 2021), donanım test yataklarına (Tam vd., 2021), kapalı ağ içi tehdit modellemelerine (He vd., 2021) veya geçmiş verileri derleyen teorik çerçevelere (Mesa vd., 2024; Pijpker ve McCombie, 2024) odaklandığı görülmektedir. Söz konusu çalışmalar tehditleri kavramsal olarak sınıflandırmada başarılı olsa da, stratejik hedeflerin dijital ayak izlerini ve dışa açık saldırı yüzeylerini gerçek zamanlı olarak saptamakta sınırlı kalmaktadır. Bu çalışma, literatürdeki simülasyon ve manuel kontrol listesi tabanlı yaklaşımların ötesine geçerek; doğrudan OSINT araçlarıyla Hürmüz Boğazı'ndaki stratejik yönetim otoritelerinin coğrafi konum ve IP altyapılarını ampirik olarak haritalandırmasıyla mevcut araştırmalardan farklılaşmakta ve alana özgün bir katkı sunmaktadır.

3. YÖNTEM

Bu çalışmada, nitel ve nicel veri toplama tekniklerinin bütünleşik olarak kullanıldığı "Keşfedici Durum Çalışması" modeli benimsenmiştir. Yin (2018) tarafından kavramsallaştırılan bu model, araştırmacının dışarıdan müdahale edemediği siber güvenlik gibi dinamik ve sınırları kesin olmayan olguların derinlemesine incelenmesi için uygun bir metodolojik çerçeve sunmaktadır. Siber tehdit istihbaratı verilerinin hızla değişen doğası, geleneksel veri toplama araçlarının ötesine geçilmesini zorunlu kılmıştır. Bu bağlamda çalışmanın metodolojik kurgusu; OSINT araçlarıyla elde edilen ampirik verilerin, Doğal Dil İşleme (NLP) algoritmaları aracılığıyla tematik olarak analiz edilmesi üzerine yapılandırılmıştır.

3.1. Evren ve Örneklem Stratejisi

Çalışmanın evrenini, küresel deniz ticaretinin stratejik düğüm noktalarında faaliyet gösteren liman otoriteleri ve denizcilik bilişim sistemleri oluşturmaktadır. Örneklem seçiminde, olasılığa dayalı olmayan yöntemlerden "Amaçlı Örnekleme" ve alt türü olan "Kritik Durum Örneklemesi" (Patton, 2015) tercih edilmiştir. Bu yaklaşım, siber tehdit potansiyelinin en yüksek olduğu aktörleri derinlemesine incelemek amacıyla kullanılmıştır.

Bu doğrultuda, küresel enerji arzının en hassas rotalarından Hürmüz Boğazı çevresinde siber altyapı hizmeti veren 10 stratejik aktör çalışmaya dâhil edilmiştir. Örneklemi oluşturan kurumlar; ulusal liman idareleri (BAE, Umman, Kuveyt, Suudi Arabistan, Katar, Bahreyn, İran), küresel OSINT veri tabanları (MarineTraffic, VesselFinder) ve bölgenin deniz güvenliğini sağlayan askeri unsurlardır (ABD 5. Filosu). Söz konusu aktörlerin seçilmesindeki temel ölçüt, boğazdaki fiziksel ve dijital veri akışını yöneten temel yasal, ticari ve askeri karar vericiler olmalarıdır. Bu durum, bölgenin siber ekosisteminin bütüncül bir şekilde analiz edilmesine olanak tanımaktadır.

3.2. Veri Toplama ve Analiz Süreci

Çalışmada, hedef kurumların dijital ayak izlerini saptamak ve elde edilen ampirik bulguları mevcut literatürle bütünleştirmek amacıyla çok katmanlı bir analiz süreci yürütülmüştür.

3.2.1. Pasif Veri Toplama Etiği ve OSINT Otomasyonu

Çalışmanın ilk aşamasında, uluslararası siber güvenlik etik standartları gereğince hedef sistemlere yönelik aktif zafiyet taramasından kaçınılmış ve tamamen pasif bilgi toplama yaklaşımı benimsenmiştir. Python tabanlı özelleştirilmiş otomasyon betikleri ile hedef kurumların alan adları üzerinden DNS sorguları gerçekleştirilmiş ve dışa açık dijital ayak izleri tespit edilmiştir. Elde edilen bulgular, Folium kütüphanesi kullanılarak uzamsal haritalama ve coğrafi konumlandırma analizine tabi tutulmuştur. Bu uzamsal analiz, kurumların idari merkezlerinden bağımsız olarak, veri egemenliğini doğrudan etkileyen asıl sunucu lokasyonlarının ve uluslararası bulut altyapılarının haritalandırılmasını sağlamıştır. Veri toplama, işleme ve görselleştirme aşamalarında yararlanılan temel araçlar ve kütüphaneler Tablo 2'de detaylandırılmıştır.

Literatürde pasif bilgi toplama süreçlerinin genellikle Shodan, Maltego, Spiderfoot ve Recon-ng gibi endüstri standardı araçlarla (Pastor-Galindo vd., 2020) veya sosyal mühendislik zafiyetlerine odaklanan Sherlock ve Creepy gibi uygulamalarla (Hassan ve Hijazi, 2018) yürütüldüğü görülmektedir. Ancak söz konusu hazır araçlar, spesifik mimari analizlerden ziyade genel zafiyet taraması veya bireysel dijital ayak izi tespiti için tasarlanmıştır. Bu çalışmada doğrudan stratejik liman otoritelerinin kurumsal ağ altyapılarına ve veri egemenliğine odaklanıldığı için, standart paket programlar yerine Python NLTK kütüphanesiyle desteklenen özelleştirilmiş Doğal Dil İşleme (NLP) algoritmaları ve "dig" komutu tabanlı spesifik sorgu betikleri tercih edilmiştir.

Tablo 2. Çalışmada Yararlanılan OSINT Araçları, Kütüphaneler ve Analiz Amaçları

Yöntem / Araç / Kütüphane	Teknik Niteliği	Çalışmadaki Spesifik Analiz Amacı
Dig	Komut Satırı Ağ Sorgu Aracı	cusnc.navy.mil (ABD 5. Filo) DNS kayıtlarını çözerek Akamai CDN arkasındaki gerçek ağ mimarisini analiz etmek.
Folium (Python)	Uzamsal Haritalama Kütüphanesi	IP tabanlı coğrafi konum verilerini koordinatlara dönüştürerek liman sunucularının mekânsal dağılımını haritalandırmak.
Google News RSS	Otomatize Veri Toplama Kaynağı	Hürmüz Boğazı'ndaki siber risklere ve liman otoritelerine yönelik 106 adet güncel haber metnini ampirik veri olarak toplamak.
NLTK (Python)	Doğal Dil İşleme (NLP) Kütüphanesi	Toplanan haber metinlerinde veri temizleme (etkisiz sözcüklerin filtrelenmesi), kök bulma ve tehdit frekans analizi gerçekleştirmek.

Kaynak: Çalışma kapsamında uygulanan OSINT metodolojisi doğrultusunda yazar tarafından oluşturulmuştur.

3.2.2. Metin Madenciliği ve Veri Üçgenlemesi

Çalışmanın ikinci aşamasında, literatürde raporlanan siber güvenlik krizleri ile sahadaki güncel tehdit ortamının örtüşme düzeyini analiz etmek amacıyla metin madenciliği yöntemlerine başvurulmuştur. Bölüm 2'de derinlemesine incelenen çalışmaların anahtar kelimelerinden yola çıkılarak "Alana Özgü Kavramsal Sözlük" inşa edilmiştir. Bu sözlük, Doğal Dil İşleme (NLP) algoritmalarıyla entegre edilerek siber tehdit söylem analizi gerçekleştirilmiştir.

Elde edilen ampirik bulguların geçerliliğini ve akademik güvenilirliğini en üst düzeye çıkarmak amacıyla Denzin (1978) tarafından kavramsallaştırılan "Veri Üçgenlemesi" stratejisi uygulanmıştır. Söz konusu doğrulama stratejisi kapsamında; hedef sistemlerin IP adres konumları, İnternet Servis Sağlayıcı (ISP) altyapıları ve sunucu başlık (HTTP header) yanıtları karşılıklı olarak teyit edilmiş, böylece tekil veri kaynaklarından doğabilecek metodolojik sapmaların önüne geçilmiştir.

Şekil 1. Araştırmanın Metodolojik Akış Şeması ve OSINT Çerçevesi

Kaynak: Çalışma kapsamında uygulanan OSINT metodolojisi doğrultusunda yazar tarafından oluşturulmuştur.

4. ANALİZ VE BULGULAR

Bu bölümde, geliştirilen OSINT otomasyonu ve NLP algoritmaları aracılığıyla elde edilen ampirik veriler sunulmaktadır. Çalışma bulguları; siber altyapı matrisi, mekânsal haritalama ve kavramsal yoğunluk analizleri olmak üzere üç temel eksende yapılandırılmıştır.

4.1. Stratejik Otoritelerin Siber Altyapı ve Konum Analizi

Araştırma kapsamında Hürmüz Boğazı ve çevresindeki 10 stratejik aktörün dışa açık dijital varlıkları üzerinde siber keşif çalışmaları yürütülmüştür. Yapılan DNS ve HTTP başlık (header) analizleri, kurumların veri barındırma stratejilerinde ciddi farklılıklar olduğunu ortaya koymuştur. Elde edilen teknik veriler, karşılaştırmalı olarak Tablo 3'te sunulmuştur.

Tablo 3. Stratejik Otoritelerin OSINT Tabanlı Siber Altyapı Matrisi

Kurum	**Domain**	**IP Adresi**	**Ülke**	**ISP**	**Sunucu Teknolojisi**
İran Limanlar Kurumu	pmo.ir	Maskelenmiş	Tespit Edilemedi	Tespit Edilemedi	Tam Maskeleme / WAF Blokajı
BAE DP World Limanı	dpworld.com	162.159.141.157	Kanada	Cloudflare, Inc.	Cloudflare CDN
Umman Limanları	asyad.om	77.83.61.24	Umman	OMANIA	Maskelenmiş
Kuveyt Liman İdaresi	kpa.gov.kw	20.254.225.239	İngiltere	Microsoft Corp.	Apache
Suudi Arabistan Limanları	mawani.gov.sa	212.70.48.27	Suudi Arabistan	Atheer Jeraisy	Bağlantı Reddedildi (WAF)
Katar Liman Yönetimi	mwani.com.qa	20.173.78.81	Katar	Microsoft Corp.	Maskelenmiş
Bahreyn Limanları	mtt.gov.bh	108.132.42.90	İrlanda	BellSouth.net Inc.	Maskelenmiş
MarineTraffic	marinetraffic.com	104.18.9.70	Kanada	Cloudflare, Inc.	Cloudflare CDN
VesselFinder	vesselfinder.com	159.69.101.70	Almanya	Hetzner Online	Bağlantı Reddedildi (WAF)
ABD 5. Filosu (Bahreyn Üssü)	cusnc.navy.mil	23.53.35.198*	ABD	Akamai Int. B.V.	AkamaiGHost

Kaynak: Geliştirilen OSINT metodolojisi doğrultusunda yazar tarafından oluşturulmuştur.

Not (*): Tabloda ABD 5. Filosu'na ait cusnc.navy.mil alan adı için tespit edilen IP adresi (23.53.35.198) ile standart ICMP sorgularından elde edilen adresler arasında yapısal bir farklılık bulunmaktadır. Hedefin küresel bir İçerik Dağıtım Ağı (CDN) olan Akamai arkasında konumlandırılması ve dinamik Geo-DNS yönlendirmesi kullanması bu durumun temel nedenidir. Standart ICMP sorguları, coğrafi

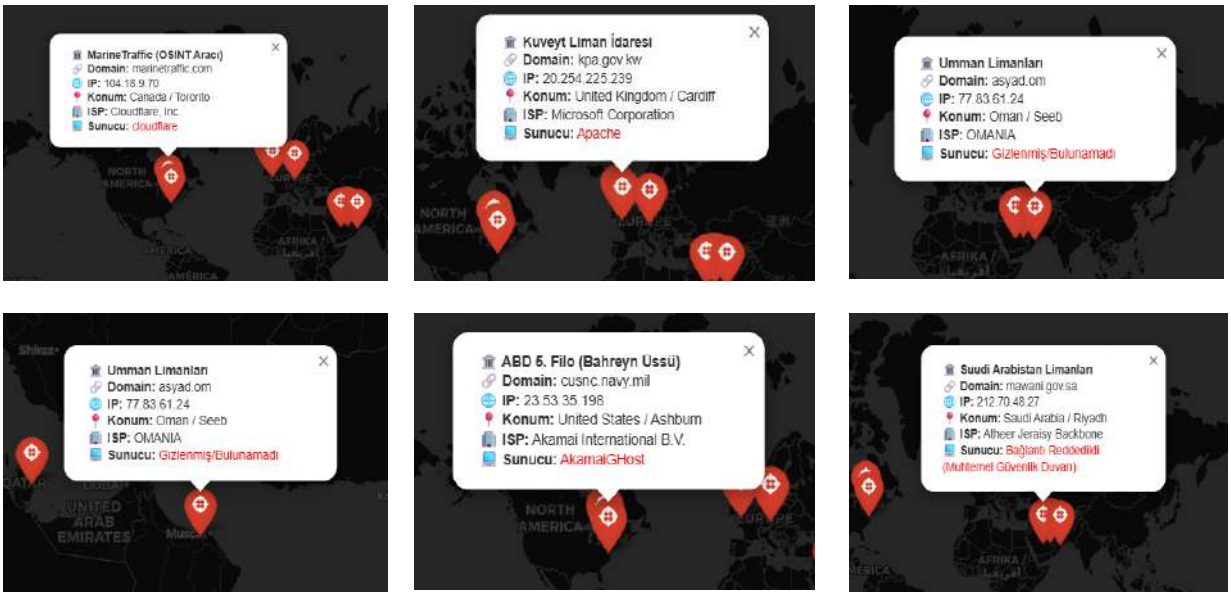
konuma bağlı olarak en düşük gecikmeyi sunan yerel uç sunuculara çözümlenirken; bu çalışmada dig komutu, ters DNS (Reverse DNS) kayıtları ve geçmiş IP log analizleri bütünleştirilerek hedefin CDN arkasındaki maskelenmiş asıl düğümüne (ABD lokasyonlu) ulaşılmıştır. Bu bulgu, askeri otoritelerin dijital varlıklarını korumak amacıyla kullandığı katmanlı ağ mimarilerinin karmaşıklığını somut bir şekilde ortaya koymaktadır.

4.2. Mekânsal Dağılım ve Veri Egemenliği Haritalaması

Kurumların siber altyapılarını coğrafi olarak görselleştirmek amacıyla Python tabanlı Folium kütüphanesinden yararlanılmıştır. Çalışma kapsamında, İran'ın uyguladığı katı siber izolasyon politikası nedeniyle tam maskeleme yapan altyapısı dışındaki 9 hedefin konumu haritalandırılmıştır. Ancak, görsel karmaşayı önlemek ve siber güvenlik stratejilerindeki bölgesel zıtlıkları net bir şekilde vurgulamak amacıyla, bu hedefler arasından seçilen 6 kritik otoritenin detaylı mekânsal görünümleri sunulmuştur.

Seçili haritalar incelendiğinde; Kuveyt ve Katar gibi Körfez aktörlerinin kritik operasyonel verilerini Avrupa merkezli dış bulut altyapılarında barındırdığı saptanmıştır. Bu tablo, söz konusu aktörler açısından siber güvenlikte "Veri Egemenliği" zafiyetine işaret etmektedir. Buna karşın, Umman ve Suudi Arabistan'ın dijital varlıklarını kendi ulusal sınırları içerisinde barındırarak dijital altyapıda millileşme ve ulusal güvenlik izolasyonu stratejisini tercih ettiği görülmektedir.

Siber çatışmaların asimetrik doğası ve tedarik zinciri riskleri göz önüne alındığında, siber altyapıların ve veri merkezlerinin yerlileştirilmesi; kriz anlarında yabancı servis sağlayıcıların uygulayabileceği veri blokajlarına veya siber istihbarat tehditlerine karşı en kritik savunma hattını oluşturmaktadır. Bu bağlamda, ABD 5. Filosu'nun fiziksel olarak Bahreyn'de konuşlanmış olmasına rağmen tüm dijital trafiğini askeri düzeydeki AkamaiGHost ağı üzerinden doğrudan ABD ana karasına yönlendirmesi çalışmanın en çarpıcı bulgularından biridir. Bu mimari yönlendirme, askeri düzeyde operasyonel güvenliğin ancak tam bir veri egemenliği ve dijital millileşme stratejisiyle tesis edilebileceğinin en somut ampirik kanıtını sunmaktadır.



Şekil 2. Seçilmiş Stratejik Otoritelerin Coğrafi Konum Haritaları

Kaynak: Yazar tarafından Python (Folium) kullanılarak OSINT verileriyle oluşturulmuştur.

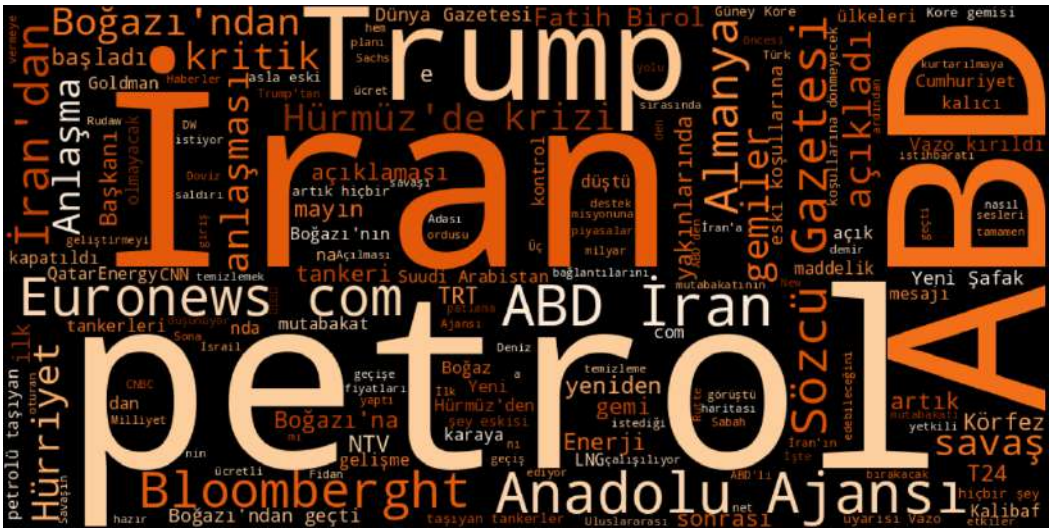
4.3. Metin Madenciliği ve Jeopolitik Söylem Analizi

OSINT sürecinin ikinci aşamasında, sahadaki siber-fiziksel tehdit algısını ampirik olarak ölçmek amacıyla metin madenciliği yöntemlerine başvurulmuştur. Veri kaynağı olarak Google News RSS beslemelerinin tercih edilmesinin temel gerekçesi; bu altyapının küresel ölçekteki on binlerce uluslararası haber otoritesini tek bir merkezde derlemesi ve bölgeye yönelik makro düzeydeki medya söylemini geniş ölçekli bir biçimde yansıtabilmesidir. Geliştirilen otomasyon betiği, API kısıtlamalarına veya sorgu limitlerine tabi olmadan belirlenen anahtar kelime kombinasyonları üzerinden toplam 106 adet güncel haber metnini derleyerek analiz veri tabanına aktarmıştır.

Elde edilen metinsel veri seti, Python (Pandas) ortamında yapılandırıldıktan sonra Terim Frekansı analizine tabi tutulmuştur. Bu analizdeki temel amaç, ham metin kütlesinin içerdiği anlamsal örüntüleri nicel veri matrislerine dönüştürmektir. Analiz öncesinde, Bölüm 3.2.2'de aşamaları sunulan metin ön işleme mimarisine tam uyumlu olarak; metinler anlamsal birimlerine ayrıştırılmış, noktalama işaretleri ile URL adresleri temizlenmiş ve anlamsal değer taşımayan Türkçe etkisiz kelimeler (stopwords) veri setinden elenmiştir. Veri toplama sürecinde Türkiye merkezli bir ağ düğümü (node) kullanıldığı için, algoritmik olarak yerel kaynaklara (TRT, Anadolu Ajansı vb.) doğal bir öncelik tanınmıştır. Ayrıca, haber başlıklarındaki anlamsal bütünlüğü ve haberin bağlamını korumak adına kök bulma (stemming) işlemi uygulanmamış; "Boğazı'ndan" gibi ifadeler orijinal çekim ekleriyle veri setinde muhafaza edilmiştir.

Bölgedeki tehdit algısını görselleştirmek amacıyla oluşturulan Şekil 3, jeopolitik söylemin "petrol", "tanker", "Trump", "İran", "ABD" ve "gemi" kavramları etrafında yoğunlaştığını nicel olarak ortaya

koymaktadır. Bu ampirik bulgu, denizcilikte siber güvenliğin yalnızca soyut bir bilişim altyapısı sorunu olmadığını; doğrudan küresel enerji arzı, deniz lojistiği ve fiziksel tedarik zinciri güvenliği jeopolitiğiyle entegre bir ulusal güvenlik meselesi olduğunu kanıtlamaktadır.



Şekil 3. OSINT Verilerine Dayalı Siber-Fiziksel Tehdit Kelime Bulutu

Kaynak: Yazar tarafından Ocak – Haziran 2026 döneminde Google News platformu üzerinden derlenen veriler kullanılarak oluşturulmuştur.

4.4. İnsan ve Strateji Boyutu: Sosyal Mühendislik, Dijital Farkındalık ve Millileşme

Denizcilik sektöründe yaşanan dijital dönüşüm; Liman 4.0 konseptinin, akıllı vinçlerin, konteyner takip sistemlerindeki IoT sensörlerinin ve AIS cihazlarının entegrasyonuyla operasyonel kapasiteyi en üst seviyeye taşımıştır. Bununla birlikte, söz konusu teknolojik atılım beraberinde yönetilmesi zor güvenlik risklerini de getirmektedir. Siber güvenlik literatüründe sosyal mühendislik modelleriyle vurgulandığı üzere (Mitnick ve Simon, 2002; Hadnagy, 2018), en karmaşık güvenlik mimarileri dahi sistemin en zayıf halkası olan "insan faktörüne" yenik düşebilmektedir. Geleneksel iş akışlarının halen belirleyici olduğu denizcilikte, personelin dijital okuryazarlık seviyesinin düşük kalması kritik bir zafiyet vektörü oluşturmaktadır. Liman personeline veya gemi mürettebatına yönelik standart bir oltalama (phishing) saldırısı ya da sosyal medya üzerinden gerçekleşen küçük ölçekli bir veri sızıntısı, tehdit aktörleri için stratejik bir istihbarat kaynağına dönüşebilmektedir. Bu bağlamda, Uluslararası Denizcilik Örgütü (IMO) ve ISPS Kodu çerçevesindeki denetimlerin (IMO, 2003) yalnızca fiziksel güvenlik önlemlerine değil; zorunlu siber hijyen eğitimlerine, periyodik oltalama tatbikatlarına ve personel farkındalığını ölçecek simülasyonlara odaklanması operasyonel bir zorunluluk haline gelmiştir.

Bölgesel krizlerde ve siber savaş senaryolarında, teknik savunma mekanizmalarının ötesinde "altyapıda millileşme" konusu kritik bir ulusal güvenlik önceliğine dönüşmektedir. Asimetrik siber çatışmaların doğası, donanım veya yazılım tedarikinde dışa bağımlı olan sistemleri hedef almaya son derece müsaittir. Bunun en çarpıcı örneği, 2017 yılında küresel çapta yaşanan NotPetya krizidir. Dışarıdan

tedarik edilen bir yazılıma entegre edilmiş arka kapı (backdoor) üzerinden yayılan siber saldırı, dünyanın en büyük denizcilik şirketlerinden Maersk'in tüm lojistik operasyonlarını günlerce sekteye uğratmıştır (Perlroth vd., 2017). Bu vaka, teknolojik dışa bağımlılığın tedarik zinciri güvenliğine verebileceği zararın en somut kanıtıdır.

Meselenin bir diğer stratejik boyutu ise fiziksel altyapı güvenliğidir. Küresel dijital trafiğin büyük bir kısmı uydularla değil, okyanusların ve deniz boğazlarının tabanına döşenmiş devasa fiber optik ağlarla taşınmaktadır (Starosielski, 2015). Hürmüz Boğazı ve Marmara Denizi gibi kritik geçiş güzergâhlarında bulunan bu hatlar, Asya ile Avrupa arasındaki veri akışının en hayati koridorlarıdır. Sonuç olarak, denizcilik siber güvenliği salt bir yazılım veya ağ sorunu olarak değerlendirilemez. Yabancı menşeli güvenlik ürünlerinin donanımsal veya yazılımsal istihbarat araçlarına dönüşebildiği günümüz konjonktüründe; kritik veri trafiğini filtreleyen yerli WAF sistemlerinin devreye alınması ve limanlara ait operasyonel verilerin sınır ötesi bulut sunucuları yerine doğrudan ulusal veri merkezlerinde barındırılması, veri egemenliğinin tesis edilmesi açısından atılması gereken en elzem adımdır.

5. SONUÇ VE ÖNERİLER

Bu çalışma, küresel deniz ticaretinin ve enerji arzının en kritik düğüm noktası olan Hürmüz Boğazı'ndaki denizcilik otoritelerinin siber güvenlik duruşlarını OSINT yöntemleriyle analiz ederek literatürdeki ampirik veri boşluğunu doldurmuştur. Geleneksel anket ve simülasyon temelli yaklaşımların ötesine geçilerek, stratejik kurumların gerçek zamanlı dışa açık saldırı yüzeyleri, geliştirilen özelleştirilmiş otomasyon betikleriyle haritalandırılmıştır.

Elde edilen bulgular, stratejik otoritelerin siber güvenlik altyapılarında "veri egemenliği" ile "dış bulut bağımlılığı" arasında belirgin bir ikilem yaşandığını göstermektedir. İncelenen 10 stratejik hedefin altyapı matrisleri; bazı Körfez ülkelerinin veri esnekliği ve dağıtık hizmet aksatma (DDoS) koruması amacıyla uluslararası bulut sağlayıcılarına yöneldiğini, buna karşın Umman ve Suudi Arabistan gibi aktörlerin verilerini ulusal sınırlar içinde barındırarak dijital izolasyon stratejisi izlediğini ortaya koymuştur. OSINT taramalarını tamamen bloke eden otoritelerin varlığı ise, bölgedeki devlet destekli WAF mekanizmalarının katı yapılandırma stratejilerini doğrulamaktadır. Öte yandan, 106 güncel haber metni üzerinden gerçekleştirilen NLP analizi, bölgedeki siber tehdit algısının petrol, tanker ve gemi gibi doğrudan lojistik ve enerji güvenliği kavramlarıyla bütünleşik olduğunu ampirik olarak kanıtlamıştır. Bu durum, denizcilik siber güvenliğinin yalnızca bir bilişim teknolojileri sorunu değil; doğrudan operasyonel teknolojileri (OT) de kapsayan fiziksel bir tedarik zinciri ve ulusal güvenlik meselesi olduğunu göstermektedir.

Çalışma sonuçları ışığında, denizcilik sektöründeki karar vericilerin ve Güvenlik Operasyon Merkezlerinin (SOC) dışa açık saldırı yüzeylerini düzenli OSINT süreçleriyle izlemeleri, sınır ötesi veri barındırma risklerine karşı hibrit bulut mimarileri geliştirmeleri ve Avrupa Birliği'nin NIS2 Direktifi gibi proaktif siber güvenlik mevzuatlarını ulusal denizcilik stratejilerine entegre etmeleri önerilmektedir.

Bu çalışmanın temel kısıtlılığı, uluslararası siber güvenlik etik standartları gereği hedef sistemlere yönelik aktif sızma testleri yapılamaması ve bulguların belirli bir zaman dilimindeki pasif dış istihbarat verileriyle sınırlı kalmasıdır. Gelecekteki çalışmaların, geliştirilen bu metodolojik çerçeveyi Süveyş Kanalı ve Malakka Boğazı gibi diğer küresel deniz ticaret rotalarına uygulayarak kapsamlı bir küresel denizcilik siber direnç haritası oluşturması literatüre önemli bir katkı sağlayacaktır.

KAYNAKÇA

Amro, A., ve Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *International Journal of Information Security, 22*(1), 249–288. https://doi.org/10.1007/s10207-022-00638-y

Amro, A., Gkioulos, V., ve Katsikas, S. (2022). Autonomous ship security: FMECA and MITRE ATT&CK frameworks. *Marine Technology Society Journal, 56*(4), 45-60.

Androjna, A., ve Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science, 10*(02), 361-373. https://doi.org/10.7225/toms.v10.n02.w08

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., ve Guevara Carazas, F. J. (2024). Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains. *Information, 15*(11), 710. https://doi.org/10.3390/info15110710

De la Peña Zarzuelo, I., Soeane, M. J. F., ve Bermúdez, B. L. (2020). Industry 4.0 in the port and maritime industry: A literature review. *Journal of Industrial Information Integration, 20*, 100173. https://doi.org/10.1016/j.jii.2020.100173

Denzin, N. K. (1978). The research act: A theoretical introduction to sociological methods (2nd ed.). New York, NY: McGraw-Hill.

Farah, N., Akhter, S., ve Sultana, S. (2022). The impact of IoT and Big Data on maritime cybersecurity: A systematic literature review. *IEEE Access, 10*, 45000-45015.

Grispos, G., ve Mahoney, W. (2022). Sectoral challenges in maritime cybersecurity: A historical case analysis. *Computers & Security, 115*, 102600.

Gunes, B., Khan, F., ve Abbassi, R. (2021). Scenario-based risk analysis for integrated port security. *Ocean Engineering, 230*, 108900.

Gyamfi, E., ve Jurcut, A. D. (2022). AI-PAML: Machine learning for IoT network security in maritime edge computing. *Internet of Things, 18*, 100490.

Hacks, S., ve Pahl, J. (2024). HarborLang and YACRAF: Detailed attack simulations for port call operations. *Journal of Information Security and Applications, 80*, 103650.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Hoboken, NJ: John Wiley & Sons.

Hassan, N. A., ve Hijazi, R. (2018). *Open source intelligence methods and tools: A practical guide to online intelligence*. New York, NY: Apress.

He, Y., Yu, F. R., ve Zhao, N. (2021). In-network threat modeling: Markov chain and DNS rebinding for maritime IoT. *IEEE Internet of Things Journal, 8*(12), 9800-9812.

Hemminghaus, C., Bauer, J., ve Padilla, E. (2021). BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15*. https://doi.org/10.12716/1001.15.01.02

IMO. (2003). *International Ship and Port Facility Security (ISPS) Code*. London, UK: International Maritime Organization.

Jacq, O., Salazar, P. G., Parasuraman, K., Kuusijärvi, J., Gkaniatsou, A., Latsa, E., ve Amditis, A. (2021). The cyber-MAR project: First results and perspectives on the use of hybrid cyber ranges for port cyber risk assessment. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 409-414. https://doi.org/10.1109/CSR51186.2021.9527968

Kavallieratos, G., ve Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering, 8*(10), 768. https://doi.org/10.3390/jmse8100768

Keskin, O. F., Lubja, K., Bahsi, H., ve Tatar, U. (2025). Systematic Cyber Threat Modeling for Maritime Operations: Attack Trees for Shipboard Systems. *Journal of Marine Science and Engineering, 13*(4), 645. https://doi.org/10.3390/jmse13040645

Lee, C., ve Lee, S. (2023). Overcoming the DDoS attack vulnerability of an ISO 19847 shipboard data server. *Journal of Marine Science and Engineering, 11*(5), 1000. doi:10.3390/jmse11051000

Mitnick, K. D., ve Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, IN: John Wiley & Sons.

Nasr, A. N., Oruç, A., Lugo, R., Zaitseva-Pärnaste, I., ve Kujala, P. (2026). A proactive defense: An open-source intelligence (OSINT) framework for maritime cybersecurity. *IEEE Access*.

Nissov, C., Jensen, M., ve Hansen, J. (2021). Topological information flow analysis for cyber resilience in maritime systems. *IEEE Transactions on Intelligent Transportation Systems, 22*(8), 5100-5115.

Okolo, C., ve Chang, V. (2021). Supply chain resilience and maritime cybersecurity: A systematic review. *International Journal of Logistics Management, 32*(4), 1120-1145.

Oruc, A., Amro, A., ve Gkioulos, V. (2022). Potential cyber risks in integrated navigation systems using MITRE ATT&CK. *WMU Journal of Maritime Affairs, 21*(1), 85-102.

Pastor-Galindo, J., Nespoli, P., Gómez Mármol, F., ve Martínez Pérez, G. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282-10304. https://doi.org/10.1109/ACCESS.2020.2965257

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Perlroth, N., Scott, M., ve Frenkel, S. (2017, 27 Haziran). Cyberattack hits Ukraine then spreads internationally. *The New York Times*. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Pijpker, E., ve McCombie, S. (2023). Designing a ship honeynet for maritime cyber threat intelligence. *Journal of Information Security and Applications, 72*, 103400.

Pijpker, E., ve McCombie, S. (2024). Analyzing the maritime cyber attack database (MCAD) for threat actor profiling. *Marine Policy, 148*, 105400.

Pöyhönen, J. (2023). A holistic research approach to smart terminal processes and information flow. *Maritime Economics & Logistics, 25*(2), 300-320.

Pöyhönen, J., ve Lehto, M. (2023). Comprehensive port security: A system of systems approach. *International Journal of Cyber Warfare and Terrorism, 13*(1), 1-18.

Progoulakis, I., ve Nikitakos, N. (2023). Managing cyber-physical risks in port infrastructures using Bow Tie and API SRA. *Safety Science, 158*, 105950.

Puchkov, O., Lande, D., Subach, I., Boliukh, M., ve Nahornyi, D. (2021). OSINT investigation to detect and prevent cyber attacks and cyber security incidents. *Information Technology and Security, 9*(2), 209-218.

Rajaram, S., ve Benson, C. (2022). Cyber risk management and OT systems analysis for shipowners. *Maritime Policy & Management, 49*(5), 670-685.

Rohan, R. (2023). Cyber attack trends in shipping: Utilizing the Diamond Model. *Journal of Transportation Security, 16*(1), 5.

Schwarz, M., ve von Solms, R. (2022). Information security incidents in maritime: A structured expert interview study. *Computers & Security, 112*, 102500.

Shi, L., ve Zhang, J. (2023). ActSTT: A deep learning model for advanced persistent threat awareness in maritime networks. *IEEE Transactions on Information Forensics and Security, 18*, 1500-1512.

Starosielski, N. (2015). *The undersea network*. Durham, NC: Duke University Press.

Sviličić, B., Kamahara, J., Čelić, J., ve Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of Maritime Affairs, 18*(3), 509-520. https://doi.org/10.1007/s13437-019-00183-x

Tam, K., Moara-Nkwe, K., ve Jones, K. (2021, Ocak). A conceptual cyber-risk assessment of port infrastructure. *World of Shipping Portugal. An International Research Conference on Maritime Affairs* (ss. 1-23).

UNCTAD. (2023). *Review of Maritime Transport 2023*. New York, NY: United Nations Publications. https://unctad.org/system/files/official-document/rmt2023_en.pdf

Yadav, P., ve Kumar, S. (2023). Machine learning in open-source intelligence for maritime security. *Artificial Intelligence Review, 56*(4), 3100-3125.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: SAGE Publications.

EXTENDED ABSTRACT

A PROACTIVE DEFENSE APPROACH IN MARITIME CYBERSECURITY: AN OSINT-BASED EMPIRICAL MAPPING OF PORTS IN THE STRAIT OF HORMUZ

The maritime industry serves not only as the backbone of global trade but also as a strategic lifeline for the economic prosperity and national security of nations, with approximately 80% of global trade volume moving through sea lanes. This sector has transformed into a complex digital ecosystem where cyber-physical systems are intricately intertwined, driven by developments such as the Port 4.0 concept, Internet of Things (IoT) sensors, cloud-based Automatic Identification Systems (AIS), and autonomous port infrastructures. However, this technological shift has introduced a cyber-attack surface that is increasingly complex to manage. The geopolitical significance of strategic chokepoints like the Strait of Hormuz makes any potential cyber interference a threat not just to regional stability but to global energy security and economic continuity. While contemporary academic literature has explored maritime cybersecurity through theoretical frameworks, historical incident databases, and network simulations, there is a distinct lack of empirical studies that map the real-time digital footprints of strategic actors in such sensitive regions. Furthermore, as established in social engineering models, even the most sophisticated technical defense architectures remain vulnerable to the human factor. In a sector characterized by traditional operational cultures, the lack of digital awareness among port personnel and vessel crews constitutes a critical vulnerability. The persistent threat of phishing attacks aimed at port authorities, combined with operational data leaks on social platforms, creates an accessible target for Open-Source Intelligence (OSINT) actors and state-sponsored cyber threat groups.

This study addresses this fundamental gap by utilizing a proactive defense approach grounded in OSINT and Natural Language Processing (NLP). The research methodology adopts an exploratory case study model, integrating qualitative and quantitative data collection techniques through customized Python-based automations. Employing purposive sampling, the research focused on ten strategic maritime authorities and entities operating in the vicinity of the Strait of Hormuz. This sample includes the national port administrations of the United Arab Emirates (UAE), Oman, Kuwait, Saudi Arabia, Qatar, and Bahrain, alongside global OSINT databases such as MarineTraffic, and critical military elements including the U.S. 5th Fleet. The initial phase of the technical analysis involved passive reconnaissance, strictly adhering to international cybersecurity ethical standards by avoiding active penetration testing or vulnerability scans. Utilizing Python's socket and requests libraries, comprehensive DNS queries and HTTP header analyses were performed to identify the external digital footprints of these targets. The findings from this phase were subsequently subjected to spatial analysis using IP geolocation tools and Folium libraries, revealing a significant strategic dilemma between data sovereignty and cloud dependency. The analysis demonstrated that while the UAE's DP World and the Kuwait Ports Authority utilize international cloud infrastructures hosted in Canada and the United Kingdom, actors such as Oman and Saudi Arabia maintain a localized strategy by hosting critical data strictly within their national borders. Furthermore, the complete blockage of OSINT queries by the Iranian Ports and Maritime Organization, achieved through stringent Web Application Firewall (WAF) and geo-blocking configurations, serves as concrete evidence of a highly restrictive, state-sponsored proactive defense posture in the region.

Beyond software and cloud infrastructures, the necessity of nationalization in hardware and cybersecurity protocols emerged as a vital strategic finding. The asymmetric nature of modern cyber conflicts exposes severe vulnerabilities in technologically dependent supply chains. Historical regional incidents, such as the compromise of high-ranking officials via hardware backdoors embedded in imported security cameras, explicitly demonstrate the national security implications of neglecting hardware nationalization. Additionally, the strategic scope of maritime cybersecurity must expand from surface operations to subsea infrastructures. Considering that the vast majority of global digital traffic is transmitted by submarine fiber-optic cables rather than satellites, strategic maritime corridors like the Strait of Hormuz and the Sea of Marmara serve as critical data arteries. Consequently, protecting maritime cyber infrastructure inherently requires securing these low-latency subsea networks through the deployment of localized WAF systems and the utilization of national data centers to establish complete data sovereignty.

To empirically measure the regional cyber-physical threat perception, the second phase of the research employed text mining techniques. By scraping Google News RSS feeds, the automated Python scripts retrieved 106 recent news articles related to the Strait of Hormuz within the timeframe of January to

June 2026. This extensive dataset was analyzed using NLP algorithms. Following a rigorous preprocessing stage to eliminate generic stopwords, a semantic analysis was conducted. The NLP analysis confirmed that the regional geopolitical discourse is predominantly clustered around physical security terms such as "oil," "tanker," "Iran," and "ship." This mathematically substantiates that maritime cybersecurity is not merely an isolated Information Technology (IT) issue but fundamentally an Operational Technology (OT) concern intricately linked with global energy logistics and physical supply chain security. Ultimately, this research recommends that maritime authorities implement continuous attack surface monitoring using active OSINT methodologies. To mitigate vulnerabilities associated with the human factor, it is imperative to enforce rigorous personnel training standards that align with the International Maritime Organization (IMO) and the International Ship and Port Facility Security (ISPS) Code. Decision-makers must adopt hybrid cloud architectures to balance operational resilience with strict national data sovereignty requirements and integrate proactive legislative frameworks, such as the European Union’s NIS2 Directive, into their national maritime strategies. Future research should aim to apply this OSINT-based empirical methodology to other critical maritime chokepoints, contributing toward the development of a comprehensive global map of maritime cyber resilience.

Cilt: 2, Sayı: 1, 2026, Sayfa: 65-93

Yönetim Bilişim Sistemleri Derneği Dergisi

ISSN: 3108-6454

Journal of Management Information Systems Association

https://www.ybs.org.tr

YOKSAVAR PRO: CİHAZ MÜHÜRLEME TEMELLİ ÇOK KATMANLI MOBİL YOKLAMA SİSTEMİ

Ersin CINDIOĞLU[a], Berivan ÖZDEMİR[a] ve Hüseyin PARMAKSIZ[b]

Makale Bilgisi

Makale Türü
Araştırma Makalesi

Gönderim Tarihi:
20/05/2026

Kabul Tarihi:
29/06/2026

Anahtar Kelimeler:
Dijital Yoklama, BLE, NFC, Siber Güvenlik, Cihaz Mühürleme.

Özet

Bu çalışmada, üniversitelerdeki yoklama süreçlerini dijitalleştiren ve çok katmanlı güvenlik mekanizmalarıyla sahte yoklama girişimlerini engellemeyi amaçlayan bir mobil yoklama sistemi geliştirilmiştir. YOKSAVAR PRO; Bluetooth Low Energy (BLE) tabanlı mesafe doğrulaması, Near Field Communication (NFC) kart eşleştirmesi, biyometrik kimlik doğrulama, tek kullanımlık belirteç (token), cihaz mühürleme ve anlık bildirim mekanizmalarını bir araya getiren bütünleşik bir çözüm sunmaktadır. Öğretim üyesi, mobil uygulama üzerinden ders seçimini yaparak BLE yayınını başlatmakta; öğrenciler ise BLE sinyalini algıladıktan sonra NFC, biyometrik doğrulama ve tek kullanımlık belirteç adımlarını tamamlayarak yoklamaya katılmaktadır. Cihaz mühürleme mekanizması, her öğrencinin yalnızca kayıtlı mobil cihazı ve kendisine tanımlı NFC kartı ile yoklama verebilmesini sağlamaktadır. Flutter tabanlı istemci mimarisi ile Supabase ve Firebase Cloud Messaging altyapılarının birlikte kullanılması sayesinde sistem, ek donanım gerektirmeyen, tamamen mobil cihazlara dayalı, ölçeklenebilir ve maliyet etkin bir çözüm sunmaktadır. Literatürde yer alan benzer sistemlerle karşılaştırıldığında YOKSAVAR PRO, altı güvenlik katmanını tek bir yapıda bütünleştiren, uygulanabilir ve kapsamlı bir yaklaşım ortaya koymaktadır. Bu yönüyle çalışma, güvenli dijital yoklama sistemlerinin tasarımına özgün ve pratik bir katkı sağlamaktadır.

[a] Lisans Öğrencisi, Bilecik Şeyh Edebali Üniversitesi, Yönetim Bilişim Sistemleri, Bilecik/Türkiye, 5025966@ogrenci.bilecik.edu.tr, ORCID: 0009-0004-4557-0485 (Sorumlu yazar)

[a] Lisans Öğrencisi, Bilecik Şeyh Edebali Üniversitesi, Yönetim Bilişim Sistemleri, Bilecik/Türkiye, 1498304@ogrenci.bilecik.edu.tr, ORCID: 0009-0005-0243-7905

[b] Dr. Öğr. Üyesi, Bilecik Şeyh Edebali Üniversitesi, Yönetim Bilişim Sistemleri, Bilecik/Türkiye, huseyin.parmaksiz@bilecik.edu.tr, ORCID: 0000-0001-8455-5625

YOKSAVAR PRO: A MULTI-LAYER MOBILE ATTENDANCE SYSTEM BASED ON DEVICE SEALING

Article Information

Article Type
Research Article

Submission Date:
20/05/2026

Acceptance Date:
29/06/2026

Keywords: Digital Attendance, BLE, NFC, Cyber Security, Device Sealing.

Abstract

In this study, a mobile attendance system was developed to digitize attendance processes at universities and prevent fraudulent attendance attempts through multi-layered security mechanisms. YOKSAVAR PRO offers an integrated solution that combines Bluetooth Low Energy (BLE)-based proximity verification, Near Field Communication (NFC) card pairing, biometric authentication, one-time tokens, device sealing, and real-time notification mechanisms. The instructor selects a class via the mobile app to initiate the BLE broadcast; students then participate in the attendance process by completing the NFC, biometric authentication, and one-time token steps after detecting the BLE signal. The device sealing mechanism ensures that each student can participate in attendance only with their registered mobile device and the NFC card assigned to them. Thanks to the combined use of a Flutter-based client architecture with the Supabase and Firebase Cloud Messaging infrastructures, the system offers a scalable and cost-effective solution that requires no additional hardware and relies entirely on mobile devices. When compared to similar systems in the literature, YOKSAVAR PRO presents a practical and comprehensive approach that integrates six security layers into a single structure. In this regard, the study provides a unique and practical contribution to the design of secure digital attendance systems.

1. GİRİŞ

Üniversitelerde öğrenci devam durumunun etkin ve güvenilir biçimde izlenmesi, öğretim süreçlerinin planlanması, ders içi katılımın değerlendirilmesi ve akademik idari süreçlerin sağlıklı yürütülmesi açısından kritik öneme sahiptir. Devam takibi, yalnızca öğrencilerin derslere katılım düzeyinin belirlenmesini değil, aynı zamanda öğrenme çıktılarına erişim, erken dönem risk analizi ve akademik başarı ile devamlılık arasındaki ilişkinin değerlendirilmesini de mümkün kılmaktadır. Buna karşın, yükseköğretim kurumlarının önemli bir bölümünde yoklama süreçleri hâlen kâğıt tabanlı imza listeleri, sözlü yoklama ya da öğretim elemanlarının manuel kontrolüne dayalı geleneksel yöntemlerle gerçekleştirilmektedir.

Bu geleneksel uygulamalar, her ne kadar düşük maliyetli ve kolay uygulanabilir görünse de ders süresinin verimsiz kullanılmasına, insan kaynaklı hata olasılığının artmasına ve kayıtların doğruluğuna ilişkin çeşitli güvenilirlik sorunlarına neden olmaktadır. Özellikle imza taklidine açık olmaları, kayıtların sonradan değiştirilebilirliği ve verilerin merkezi bir yapıda anlık olarak işlenememesi, devam kontrol süreçlerinin şeffaflığını ve denetlenebilirliğini zayıflatmaktadır. Ayrıca, manuel yöntemlerin dijital raporlama, analiz ve karar destek sistemleriyle entegrasyonunun sınırlı olması, üniversitelerin veri odaklı akademik yönetim anlayışına geçişini zorlaştırmaktadır.

Bu bağlamda, öğrenci devam takibinin dijital, güvenli, hızlı ve doğrulanabilir teknolojilerle yeniden tasarlanması hem eğitim kalitesinin artırılması hem de akademik süreçlerin sürdürülebilir biçimde optimize edilmesi açısından önemli bir araştırma alanı olarak öne çıkmaktadır. Geliştirilecek yenilikçi çözümler, öğretim elemanlarının operasyonel yükünü azaltırken öğrenci devam verilerinin doğruluğunu artırarak daha etkin bir eğitim yönetim altyapısının oluşturulmasına katkı sağlayacaktır.

YOKSAVAR PRO, üniversitelerdeki yoklama süreçlerini mobil cihazlar aracılığıyla dijitalleştirmeyi ve sahte yoklama girişimlerini azaltmayı amaçlamaktadır. Sistemde; BLE tabanlı mesafe doğrulaması, Near Field Communication (NFC) kart eşleştirmesi, biyometrik kimlik doğrulama, tek kullanımlık belirteç (token), cihaz mühürleme ve anlık bildirim mekanizmaları birlikte kullanılmaktadır. Biyometrik doğrulama (parmak izi), yalnızca öğrencinin uygulamaya erişebilmesi amacıyla mobil cihazın yerleşik güvenlik altyapısı üzerinden gerçekleştirilmektedir. Bu süreçte herhangi bir biyometrik şablon veya ham biyometrik veri sunucuda ya da Supabase veritabanında saklanmamaktadır. Bu sayede sistem, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun özel nitelikli kişisel verilere ilişkin 6. maddesi ile veri minimizasyonu ilkesi doğrultusunda tasarlanmıştır (Kişisel Verileri Koruma Kurumu [KVKK], 2016). Böylece her öğrenci, yoklama işlemini yalnızca kendisine kayıtlı mobil cihazı ve kendisine tanımlı NFC kartı ile gerçekleştirebilmektedir.

YOKSAVAR PRO; Flutter tabanlı mobil uygulama, Supabase bulut veritabanı ve Firebase Cloud Messaging bildirim altyapısı kullanılarak tamamen mobil cihazlar üzerinde çalışacak şekilde tasarlanmıştır. Bu nedenle her sınıfa ayrıca RFID okuyucu, beacon cihazı veya yüz tanıma kamerası kurulmasına gerek duyulmamaktadır. Sınıfa yerleştirilen kamera tabanlı çözümlerde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 5. ve 6. maddeleri kapsamında açık rıza alınması ve aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir. Bu durum, söz konusu sistemlerin kurumsal ölçekte uygulanmasını zorlaştırmaktadır (KVKK, 2016). Önerilen sistem ise ek donanım, ek enerji ve ek bakım maliyeti gerektirmemesi nedeniyle Birleşmiş Milletler'in Sürdürülebilir Kalkınma Amaçlarından SDG-4 (Nitelikli Eğitim) ve SDG-9 (Sanayi, Yenilikçilik ve Altyapı) ile uyumlu bir Education 4.0 uygulaması olarak literatüre katkı sunmaktadır (United Nations, 2015). Çalışmanın temel katkısı, mevcut elektronik yoklama sistemlerinin güvenlik ve sürdürülebilirlik açısından sahip olduğu sınırlılıkları dikkate alarak ek donanım gerektirmeyen ve birden fazla doğrulama katmanını bütünleşik biçimde kullanan güvenli bir mobil yoklama sistemi önermesidir.

Çalışmanın ikinci bölümünde RFID, BLE, NFC, QR ve GPS tabanlı yoklama sistemleri kronolojik olarak incelenmiş; mevcut çalışmalar güvenlik katmanları açısından karşılaştırılmıştır. Üçüncü bölümde YOKSAVAR PRO'nun genel mimarisi, öğretim üyesi ve öğrenci süreçleri, cihaz mühürleme mekanizması, bildirim altyapısı, yönetim paneli ve veritabanı yapısı açıklanmıştır. Dördüncü bölümde, gerçek sınıf ortamında gerçekleştirilen testlerden elde edilen bulgulara yer verilmiş; beşinci bölümde ise sonuçlar, mevcut çözümlerle karşılaştırmalar ve gelecekte yapılabilecek çalışmalara yönelik öneriler tartışılmıştır.

2. LİTERATÜR ÖZETİ

Yoklama süreçlerinin dijitalleştirilmesi konusu, mobil cihazların ve kablosuz teknolojilerin yaygınlaşmasıyla birlikte 2010'lu yılların ortasından itibaren artan biçimde çalışılmaktadır. Açık erişimli akademik veri tabanı OpenAlex'te (Priem vd., 2022) "attendance system", "BLE", "NFC", "biometric" ve "mobile security" anahtar kelimeleriyle gerçekleştirilen tarama sonucunda, geleneksel yöntemlere alternatif olarak farklı elektronik yoklama sistemlerinin geliştirildiği görülmektedir. Eğitimde dijital dönüşüm ve Education 4.0 yaklaşımıyla birlikte Internet of Things (IoT) ve bulut hizmetlerinin eğitimde giderek daha yaygın kullanılması, bu dönüşümü hızlandırmış; geleneksel yoklama uygulamaları, RFID, BLE, NFC, QR kod ve GPS gibi teknolojilere dayalı dijital sistemlere dönüşmeye başlamıştır. Bu bölümde mevcut çalışmalar kronolojik bir sıra ile ele alınmış, her dönemin öne çıkan yaklaşımı ve sınırlılıkları değerlendirilmiştir.

İlk dönem çalışmaları arasında Noguchi vd. (2015) tarafından geliştirilen BLE beacon tabanlı Android yoklama sistemi yer almaktadır. Bu çalışma, BLE teknolojisinin yoklama amacıyla kullanılabileceğini gösteren öncü uygulamalardan biri olarak değerlendirilmektedir.

2018 yılına gelindiğinde RFID tabanlı çözümler ön plana çıkmıştır. Sezdi ve Tüysüz (2018) tarafından geliştirilen RFID tabanlı sistemde yoklama işlemleri web servisler aracılığıyla yönetilmiş ve merkezi veritabanında saklanmıştır. Aynı yıl Özcan, Saray ve Tari (2018), RFID okuyucu ve Bluetooth düşük enerji modülünü birlikte kullanarak mobil cihazlarla desteklenen bir öğrenci yoklama sistemi tasarlamıştır. Bu dönemdeki sistemlerde RFID okuyucu, Bluetooth modülü veya sınıfa kurulması gereken ek donanımlar öne çıkmakta olup, bu durum sınıf başına ek kurulum maliyeti oluşturmaktadır. Güvenlik açısından önemli bir uyarı Kim vd. (2018) tarafından gerçekleştirilen sinyal taklit saldırısı çalışmasıyla literatüre kazandırılmıştır. Bu çalışmada BLE beacon tabanlı elektronik yoklama sistemlerinin sinyal taklidi ve tekrar saldırılarıyla atlatılabileceği gösterilmiş; böylece yalnızca BLE sinyaline dayanan doğrulama yaklaşımlarının güvenlik açısından sınırlı kalabileceği ortaya konmuştur.

2020'li yılların başında akıllı telefon merkezli yaklaşımlar yaygınlaşmıştır. Alcantara vd. (2022), BLE tabanlı akıllı yoklama sisteminin uygulama ve performans analizini incelemiş; Chiang vd. (2022) ise GPS ve NFC teknolojilerini akıllı telefonlar üzerinden birleştiren bir yoklama izleme sistemi geliştirmiştir. Bu yaklaşımlar ek donanım ihtiyacını azaltmakla birlikte, iç mekânda GPS doğruluğunun düşük olması nedeniyle güvenilirliğini yitirmekte veya yalnızca tek bir doğrulama katmanına dayanmaktadır.

2024 yılında Du vd. (2025), UST ortaokulu öğrencileri için NFC teknolojilerine dayalı güvenli ve otomatik bir yoklama takip sistemi sunmuştur. Bu çalışma, NFC tabanlı sistemlerin öğrenci takibinde kullanılabilirliğini göstermesi açısından önemlidir. Ancak NFC tabanlı sistemlerde kart, okuyucu veya kurumsal kart altyapısı gibi bileşenlere ihtiyaç duyulabilmektedir.

2025 yılına gelindiğinde literatürün belirgin biçimde çeşitlendiği görülmektedir. BLE tarafında Jain (2025), öğretmen cihazının oturum bilgisi yayınladığı ve öğrenci cihazlarının bu yayını algılayarak katılım sürecine dahil olduğu ölçeklenebilir bir BLE tabanlı yoklama yaklaşımı önermiştir. Nagarajan vd. (2025), giyilebilir BLE cihazları üzerinden çalışan bir yoklama yapısını incelemiş; Munivrana vd. (2025) ise Smarttendance adlı BLE tabanlı gerçek zamanlı öğrenci yoklama uygulamasını sunmuştur. NFC tarafında Phan vd. (2025), IoT tabanlı bir NFC öğrenci yoklama sistemi üzerinde yapay sinir ağları ve rastgele orman algoritmalarını karşılaştırmıştır. GPS tarafında Madhu vd. (2025), GPS konum doğrulama, BLE beacon tespiti ve yüz doğrulama bileşenlerini içeren mobil yoklama yaklaşımını ele almıştır. QR kod tarafında ise Surve vd. (2025), Flutter ile geliştirilen bir QR kod yoklama otomasyonu sunmuştur. Bu çalışmalar, 2025 sonrasında yoklama sistemlerinin yalnızca tek bir teknolojiye değil, farklı doğrulama ve otomasyon yaklaşımlarına yöneldiğini göstermektedir.

2026 yılı çalışmalarında BLE ve QR yaklaşımları yine ön plandadır. Shaikh vd. (2026), öğretmenin mobil cihazını BLE yayıncısı olarak kullanan ve öğrenci cihazlarının BLE sinyalini algılamasına dayanan bir sistem geliştirmiştir. Patel (2026) ise konum tabanlı QR yoklama sistemi ve mobil uygulama entegrasyonunu ele almıştır. QR kod tabanlı sistemlerde uygulama kolaylığı bulunmakla birlikte, kodun ekran görüntüsüyle paylaşılması veya fiziksel sınıf içi varlığın tek başına garanti edilememesi gibi riskler devam etmektedir. Özellikle yalnızca QR kod, BLE ya da kart okutma yöntemine dayalı sistemlerde, öğrencilerin fiziksel olarak sınıfta bulunmadan da yoklama verebildiği görülmekte; bu durum ise yoklama sürecinin güvenilirliğini ve şeffaflığını olumsuz etkilemektedir (Kim vd., 2018).

Literatür genel olarak değerlendirildiğinde, elektronik yoklama sistemlerinin büyük çoğunluğunun tek ya da sınırlı sayıda doğrulama katmanına dayandığı görülmektedir. BLE tabanlı sistemler fiziksel yakınlık doğrulamasını, RFID/NFC tabanlı sistemler kart doğrulamasını, GPS tabanlı sistemler konum bilgisini, QR kod tabanlı sistemler ise hızlı katılım kaydını öne çıkarmaktadır. Buna karşın cihaz mühürleme, oturum sonrası anlık bildirim, yerel biyometrik doğrulama, tek kullanımlık token ve birden fazla doğrulama katmanının aynı akış içinde birlikte kullanılması literatürde sınırlı biçimde ele alınmıştır. Bu nedenle YOKSAVAR PRO, mevcut çalışmaların sınırlılıklarını dikkate alarak çok katmanlı, mobil cihazlara dayalı ve ek sınıf donanımı gerektirmeyen bir dijital yoklama yaklaşımı sunmaktadır.

Tablo 1. Literatürdeki Mevcut Çalışmalar

Sistem	BLE	NFC/ RFID	GPS/ Konum	Biyometrik /Yüz	Token /QR	Cihaz Mühürleme	Bildirim
Noguchi vd. (2015)	Var	–	–	–	–	–	–
Sezdi ve Tüysüz (2018)	–	RFID	–	–	–	–	–
Özcan vd. (2018)	Var	RFID	–	–	–	–	–
Kim vd. (2018)	BLE güvenlik analizi	–	–	–	–	–	–
Alcantara vd. (2022)	Var	–	–	–	–	–	–
Chiang vd. (2022)	–	Var	Var	–	–	–	–
Du vd. (2025)	–	Var	–	–	–	–	–
Jain (2025)	Var	–	–	–	–	–	–
Phan vd. (2025)	–	Var	–	–	–	–	–
Madhu vd. (2025)	Var	–	Var	Yüz doğrulama	–	–	–
Munivrana vd. (2025)	Var	–	–	–	–	–	–
Nagarajan vd. (2025)	Var	–	–	–	–	–	–
Surve vd. (2025)	–	–	–	–	QR	–	–
Shaikh vd. (2026)	Var	–	–	–	–	–	–
Patel (2026)	–	–	Var	–	QR	–	–
YOKSAVAR PRO	Var	Var	–	Var	Var	Var	Var

Çalışma kapsamında geliştirilen YOKSAVAR PRO, Tablo 1'de literatürde yer alan mevcut çalışmalarla karşılaştırılmaktadır. Karşılaştırmada; BLE tabanlı mesafe doğrulaması, Near Field Communication (NFC) kart eşleştirmesi, biyometrik kimlik doğrulama, tek kullanımlık belirteç (token), cihaz mühürleme ve anlık bildirim mekanizmaları değerlendirme ölçütü olarak dikkate alınmıştır.

Tablo 1, literatürde yer alan çalışmaların büyük çoğunluğunun tek bir doğrulama katmanına veya sınırlı sayıda kontrol mekanizmasına dayandığı görülmektedir. BLE tabanlı sistemler fiziksel yakınlık doğrulamasını merkeze alırken, RFID/NFC tabanlı sistemler kart doğrulamasına, GPS/konum tabanlı sistemler ise öğrencinin belirli bir konumda bulunup bulunmadığının denetlenmesine odaklanmaktadır. QR kod tabanlı çözümler uygulama kolaylığı sağlamakla birlikte, kodun ekran görüntüsü alınarak paylaşılabilmesi veya öğrencinin fiziksel olarak sınıfta bulunup bulunmadığının tek başına doğrulanamaması gibi güvenlik risklerini tamamen ortadan kaldıramamaktadır.

Kim vd. (2018) tarafından gerçekleştirilen çalışma, BLE beacon tabanlı elektronik yoklama sistemlerinin sinyal taklidi saldırılarına karşı savunmasız olabileceğini göstermesi bakımından önem taşımaktadır. Bu bulgu, yalnızca BLE sinyalinin algılanmasına dayalı yoklama sistemlerinde fiziksel yakınlık bilgisinin tek başına yeterli bir güvenlik ölçütü olarak değerlendirilemeyeceğini ortaya koymaktadır. Bu nedenle YOKSAVAR PRO'da BLE sinyali, yoklama sürecinin yalnızca bir doğrulama katmanı olarak ele alınmakta; NFC kart doğrulaması, biyometrik kimlik doğrulama, tek kullanımlık belirteç (token) ve cihaz mühürleme mekanizmalarıyla desteklenmektedir. Böylece,

doğrulama katmanlarından herhangi birinin aşılması durumunda sistemin bütüncül güvenlik yapısının geçersiz hâle gelmesi önlenmeye çalışılmaktadır.

RFID/NFC tabanlı bazı sistemlerde harici okuyucu, mikrodenetleyici veya kurumsal kart altyapısı gibi ek bileşenlere ihtiyaç duyulabilmektedir. Bu durum, özellikle sınıf sayısı fazla olan kurumlarda kurulum, bakım ve ölçeklendirme açısından ek maliyet oluşturabilmektedir. YOKSAVAR PRO ise öğretim üyesi ve öğrencilerin mevcut mobil cihazları üzerinden çalışacak şekilde tasarlandığı için her sınıfa ayrı RFID okuyucu, bağımsız beacon cihazı, kamera sistemi veya özel turnike altyapısı kurulmasını gerektirmemektedir. Bu yönüyle sistem, maliyet etkin ve daha kolay uyarlanabilir bir dijital yoklama yaklaşımı sunmaktadır.

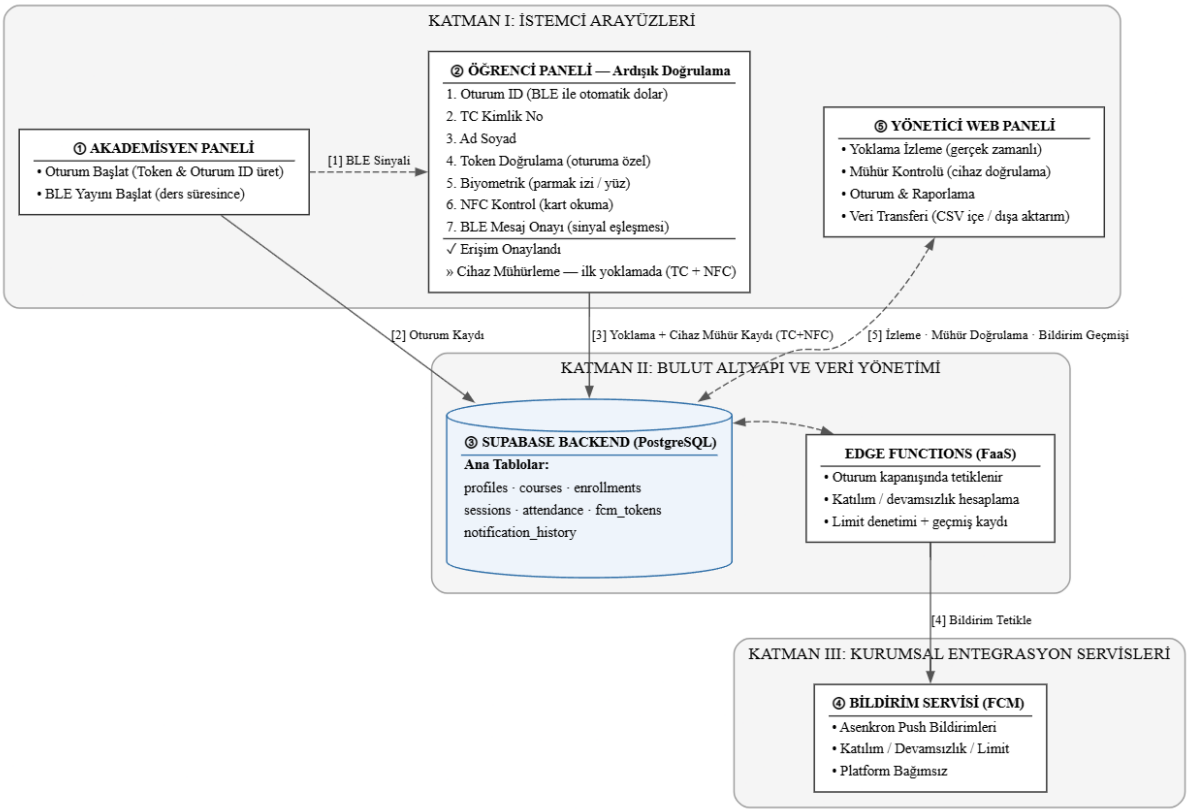
Çalışmanın bir diğer ayırt edici yönü, yoklama oturumu tamamlandıktan sonra öğrencilerin katılım durumlarına ilişkin anlık bildirim alabilmesidir. Literatürde yer alan çalışmaların önemli bir bölümü yalnızca yoklama kaydının alınmasına odaklanırken, YOKSAVAR PRO yoklama sonrasındaki bilgilendirme sürecini de sistemin ayrılmaz bir parçası hâline getirmektedir. Bu özellik, öğrencilerin devamsızlık durumlarını daha hızlı takip edebilmesine ve devam durumunun daha şeffaf bir şekilde izlenmesine katkı sağlamaktadır. Tablo 1'de görüldüğü üzere literatürde incelenen çalışmaların hiçbirinde BLE tabanlı mesafe doğrulaması, NFC kart eşleştirmesi, biyometrik kimlik doğrulama, tek kullanımlık belirteç (token), cihaz mühürleme ve anlık bildirim mekanizmalarının tamamı aynı sistem içinde bütünleşik olarak sunulmamaktadır. Bu bağlamda YOKSAVAR PRO, mevcut yaklaşımlardaki tek doğrulama yöntemine dayalı sınırlılıkları azaltmayı amaçlayan, çok katmanlı ve bütünleşik bir dijital yoklama sistemi olarak öne çıkmaktadır.

3. YÖNTEM

Bu çalışma, bilgi sistemlerinde yaygın olarak kullanılan Tasarım Bilimi Araştırması yaklaşımını kullanarak, eğitim ortamında güvenliğe ağırlık veren bir mobil devam sistemi tasarımı, geliştirilmesi ve test edilmesine odaklanmaktadır. Çalışma şu araştırma sorusunu ele almaktadır: “Ek donanım gerektirmeyen ve çok katmanlı güvenlik sistemine sahip bir mobil devam sistemi, üniversitelerde sahte devam kayıtlarını ve veri güvenilirliği sorunlarını ne ölçüde en aza indirebilir?” Çalışma, dört temel tasarım hedefi belirlemektedir: BLE tabanlı yakınlık doğrulaması, NFC kart eşleştirme, biyometrik kimlik doğrulama, tek kullanımlık jetonlar, cihaz mühürleme ve anlık bildirimlerin entegrasyonu; bunların tümü, kurumlar için ekstra donanım maliyetlerinden kaçınmak amacıyla mevcut akıllı telefonlar üzerinden çalışmaktadır. Kişisel Verilerin Korunması Hakkında 6698 Sayılı Kanun’a (KVKK) uygunluk sağlanmaktadır. Sistem, başarı oranı, performans ve kullanıcı kabulüne odaklanılarak gerçek sınıf veya laboratuvar ortamlarında test edilecek ve üç temel bileşenden oluşacaktır: öğrenciler ve öğretim üyeleri için YOKSAVAR PRO mobil uygulaması, iş mantığı için Edge Functions içeren bir Supabase arka uç altyapısı ve izleme ile raporlama için bir yönetim paneli.

Değerlendirme, pratik senaryolardaki etkinliğini ölçmek amacıyla işlevsel testler ve performans ölçütlerini içermektedir.

Yöntem kapsamında öncelikle üniversitelerde kullanılan geleneksel ve elektronik yoklama süreçlerinde karşılaşılan güvenlik, doğrulama ve sürdürülebilirlik problemleri ele alınmıştır. Bu problemlere çözüm olarak BLE, NFC, biyometrik doğrulama, tek kullanımlık token, cihaz mühürleme ve anlık bildirim mekanizmalarını bir arada kullanan çok katmanlı bir dijital yoklama mimarisi tasarlanmıştır. Geliştirilen YOKSAVAR PRO; öğretim üyesinin dersi mobil uygulama üzerinden başlatıp oturum boyunca BLE yayını yapması, öğrencinin ise sırasıyla BLE yakınlık doğrulaması, NFC kart eşleştirmesi, biyometrik kimlik kontrolü ve tek kullanımlık token adımlarını tamamlayarak yoklama işlemini gerçekleştirmesi şeklinde uçtan uca bir akışla çalışmaktadır. Bu aşamaların ardından bulut veritabanına yazılan kayıtlar, Edge Function aracılığıyla işlenir ve hem öğrenciye hem de akademisyene anlık bildirim olarak iletilmektedir. Bu yapıya ait Graphviz ile oluşturulan büyük resim Şekil 1'de gösterilmiştir.



Şekil 1. YOKSAVAR PRO Büyük Resim

Çalışmanın yazılım altyapısında, Google tarafından geliştirilen Dart programlama dili üzerine inşa edilmiş ve çapraz platform (cross-platform) mobil geliştirme framework'ü olan Flutter tercih edilmiştir. Flutter, tek kod tabanıyla hem Android hem iOS için derlenebilmesi sayesinde geliştirme süresini kısaltmakta ve farklı cihaz markaları arasında tutarlı bir arayüz sunmaktadır (Google LLC, 2023). Bu özellikler, Education 4.0 odaklı mobil uygulamalarda hem hızlı prototipleme hem de geniş

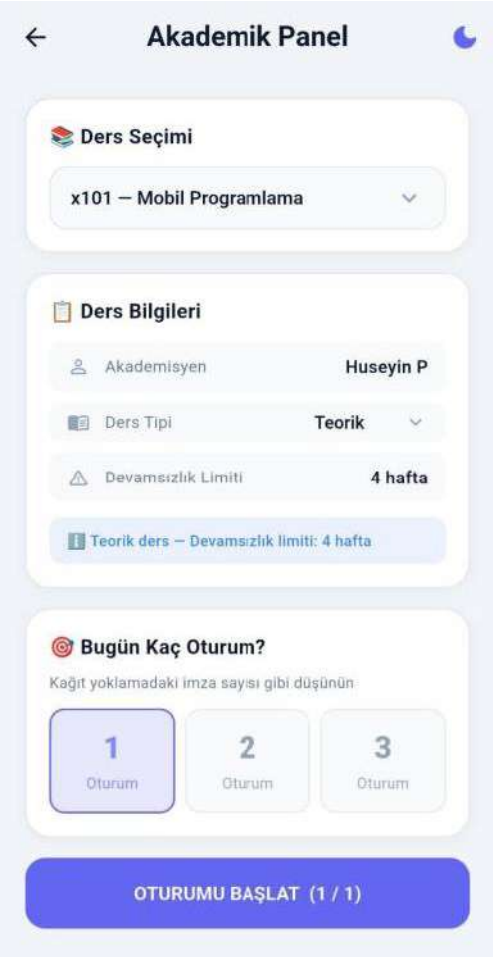
cihaz yelpazesinde sorunsuz çalışabilme açısından önemli bir avantaj sağlamaktadır. BLE iletişimi için flutter_blue_plus, NFC işlemleri için nfc_manager, biyometrik doğrulama için local_auth ve cihaz mühürlemede kullanılan donanım kimlik bilgileri için device_info_plus kütüphaneleri kullanılmıştır. device_info_plus kütüphanesi Android cihazlarda ANDROID_ID, model ve üretici bilgisi; iOS cihazlarda ise identifierForVendor değeri başta olmak üzere cihaza özgü donanım tanımlayıcılarını toplayarak öğrencinin cihazına birebir eşleşen bir yazılımsal parmak izi oluşturmaktadır (Flutter Community, 2024).

Veri katmanında Supabase tercih edilmiştir. Supabase, açık kaynaklı bir Backend-as-a-Service (BaaS) çözümü olup PostgreSQL veritabanını satır düzeyinde güvenlik (Row Level Security – RLS) mekanizmasıyla birlikte sunmaktadır. Yoklama oturumu kapatıldıktan sonra çalışan iş mantığı, Supabase Edge Functions üzerinde Function-as-a-Service (FaaS) mimarisi kullanılarak yürütülmektedir (Supabase, 2022). Adhoni vd. (2025), FaaS yaklaşımının özellikle öğrenci yoklama web uygulamalarında ölçeklenebilirlik ve verimlilik açısından önemli kazanımlar sağladığını göstermiştir. YOKSAVAR PRO'da da aynı mimari yaklaşım benimsenmiştir.

Bildirim altyapısı için Firebase Cloud Messaging (FCM) tercih edilmiştir. FCM, anlık bildirimleri ücretsiz ve düşük gecikme süresiyle ileterek Short Message Service (SMS) tabanlı bildirim sistemlerinde ortaya çıkan abonelik ve mesaj başına ücretlendirme maliyetlerini ortadan kaldırmaktadır. Bu sayede, çok sayıda öğrenciye hizmet veren yükseköğretim kurumları için daha sürdürülebilir ve maliyet etkin bir bildirim altyapısı sunulmaktadır. Bu bileşenler, sistem içerisinde birbirinden bağımsız yapılar olarak değil, aynı yoklama sürecini tamamlayan bütünleşik bir iş akışının parçaları olarak çalışmaktadır. Öğretim üyelerinin mobil uygulama üzerinden yoklama oturumunu başlatmasıyla başlayan süreç; öğrencinin doğrulama adımlarını tamamlaması, yoklama bilgilerinin veritabanına kaydedilmesi ve oturum sonrasında ilgili bildirimlerin iletilmesiyle tamamlanmaktadır. Bu yapı sayesinde öğretim üyesi, öğrenci, veri işleme ve bildirim katmanları tek bir uçtan uca iş akışı içerisinde bütünleşik olarak yönetilmektedir. Söz konusu iş akışı; öğretim üyesi süreci, öğrenci doğrulama süreci, cihaz mühürleme mekanizması, bildirim sistemi, yönetim (admin) web paneli ve veritabanı mimarisi başlıkları altında aşağıda açıklanmaktadır.

3.1. Öğretim Üyesi Süreci

Öğretim elemanı, mobil uygulama üzerinden önceden tanımlanmış dersler arasından ilgili dersi seçerek yoklama oturumunu başlatmaktadır. Ders seçimi yapıldığında ders adı, ders türü, sorumlu öğretim elemanı bilgisi ve devamsızlık limiti sistem tarafından otomatik olarak görüntülenmektedir. Öğretim elemanı, ilgili güne ait oturum sayısını belirledikten sonra, Şekil 2'de temsili olarak gösterilen yoklama oturumunu başlatmaktadır.



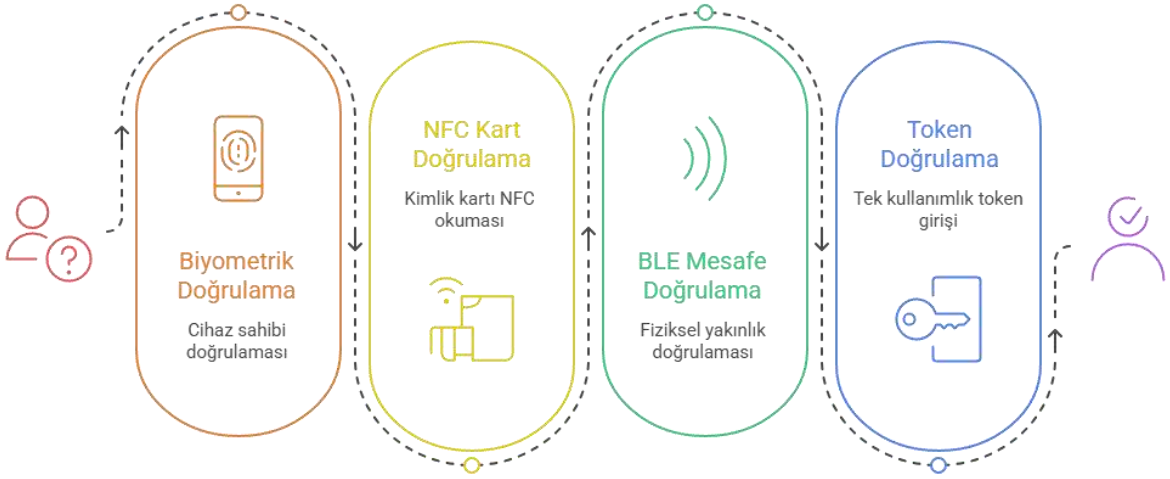
Şekil 2. Akademisyen Paneli: Ders Seçimi ve Canlı Oturum Görünümü

Oturum başlatıldığında sistem benzersiz bir session_id üretmekte ve öğretim üyeslerinin mobil cihazı flutter_blue_plus kütüphanesi aracılığıyla BLE yayıncısı olarak çalışmaya başlamaktadır. Yayın içerisinde session_id ve oturuma özel Universally Unique Identifier (UUID) değeri bulunmakta, bu bilgi sınıf ortamındaki öğrenci cihazları tarafından algılanarak yoklama sürecinin ilk fiziksel yakınlık doğrulama katmanını oluşturmaktadır.

3.2. Öğrenci Süreci

Öğrenciler, mobil uygulamaya giriş yaptıktan sonra yoklama verebilmek için çok katmanlı bir doğrulama sürecini tamamlamaktadır. Sistemde öğrenci tanımlayıcısı olarak okul numarası esas alınmaktadır. Ancak bu çalışmanın uygulandığı üniversitede öğrenciler T.C. kimlik numarası ile tanımlandığından, giriş işlemi bu numara üzerinden gerçekleştirilmektedir. Bu süreç, öğrencinin yalnızca sisteme erişmesini değil, aynı zamanda kimliğinin doğrulanmasını, kendisine tanımlı NFC kartının doğrulanmasını, fiziksel olarak ders ortamında bulunduğunun belirlenmesini ve ilgili yoklama oturumuna gerçekten katıldığının doğrulanmasını amaçlamaktadır. Bu yönüyle öğrenci doğrulama süreci, tek bir doğrulama yöntemine dayanmayan, birbirini tamamlayan güvenlik katmanlarından oluşan çok aşamalı bir yapı sunmaktadır.

Şekil 3'te gösterildiği üzere öğrenci doğrulama süreci; biyometrik kimlik doğrulama, NFC kart doğrulaması, BLE tabanlı mesafe doğrulaması ve tek kullanımlık belirteç (token) doğrulaması olmak üzere dört temel adımdan oluşmaktadır. Bu adımların her biri, öğrencinin yoklama işlemini güvenli ve geçerli bir biçimde tamamlamasına katkı sağlamaktadır.



Şekil 3. Öğrenci Doğrulama Süreci

Kaynak: Yazarlar tarafından Napkin AI (Napkin AI, 2024) kullanılarak oluşturulmuştur.

İlk aşama olan biyometrik kimlik doğrulama adımında, öğrencinin mobil cihazında tanımlı parmak izi doğrulama yöntemi kullanılmaktadır. Bu adımın temel amacı, yoklama işlemini başlatan kişinin gerçekten cihazın kayıtlı kullanıcısı olup olmadığını doğrulamaktır. Böylece, öğrenciye ait mobil cihazın başka bir kişi tarafından kullanılarak yoklama verilmesi engellenmeye çalışılmaktadır. Ayrıca biyometrik doğrulama, cihazın yerleşik güvenlik altyapısı üzerinden gerçekleştirildiğinden herhangi bir biyometrik veri sunucuya aktarılmamakta; sistem yalnızca doğrulama sonucundan yararlanmaktadır.

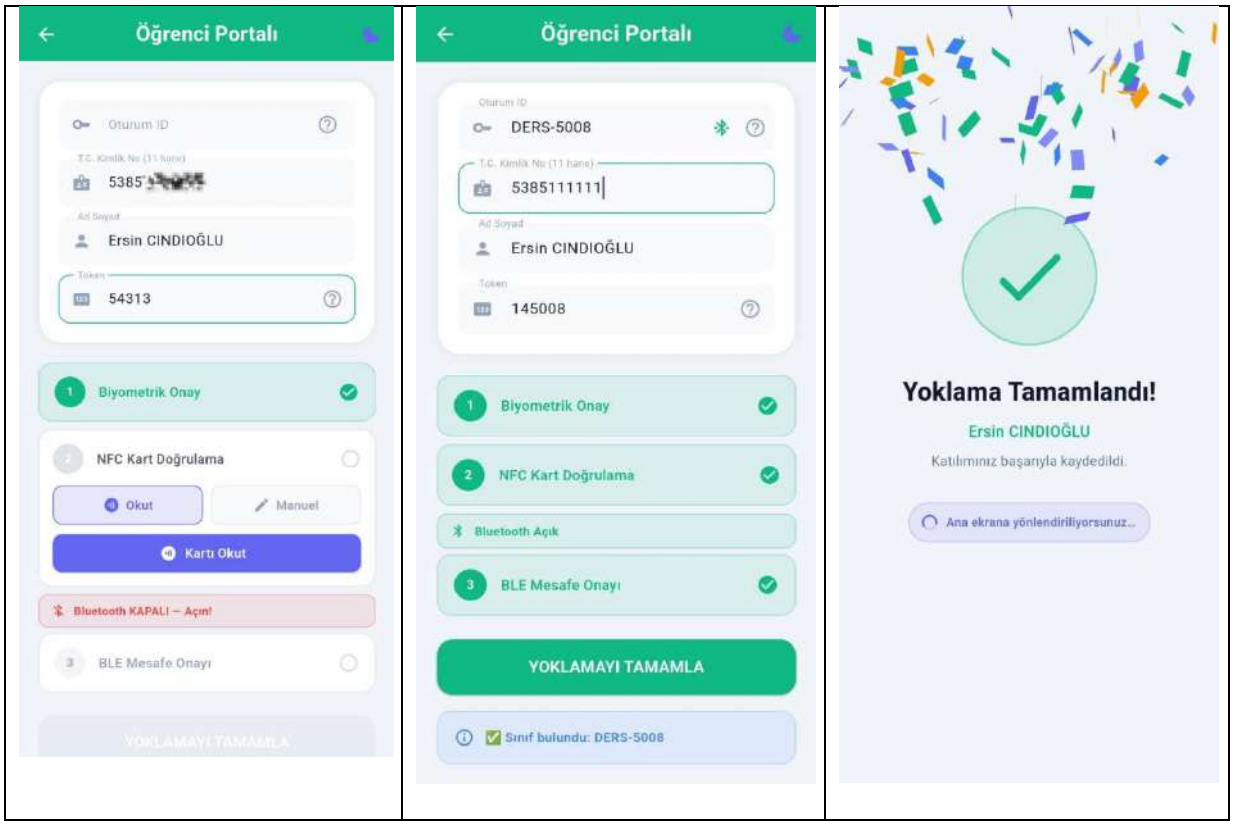
İkinci aşama olan NFC kart doğrulama adımında, öğrencinin kimlik kartının veya kendisine tanımlanmış NFC etiketinin mobil cihaz aracılığıyla okutulması sağlanmaktadır. Sistem, karttan elde edilen Unique Identifier (UID) değerini, veritabanında öğrenci profiliyle ilişkilendirilmiş kayıtlı NFC UID bilgisiyle karşılaştırmaktadır. Eşleşme sağlandığında doğrulama süreci bir sonraki aşamaya geçmektedir. NFC desteği bulunmayan mobil cihazlarda ise kullanıcının UID bilgisini manuel olarak girmesine olanak tanınmaktadır. Öğrenci bu bilgiyi, NFC özelliğine sahip bir cihaz aracılığıyla kartını okutarak veya kurumsal kart bilgilerinden temin edebilmektedir.

Mükerrer veri girişini önlemek amacıyla girilen T.C. kimlik numarası, ad ve soyadı ile NFC UID bilgisi, shared_preferences kütüphanesi kullanılarak cihazda kalıcı olarak saklanmakta ve sonraki yoklama oturumlarında otomatik doldurma (autofill) özelliği sayesinde ilgili alanlara otomatik olarak yerleştirilmektedir. Bu sayede öğrencinin her yoklama oturumunda aynı bilgileri yeniden girmesine

gerek kalmamaktadır. Bu doğrulama adımı, öğrencinin yalnızca kendisine tanımlı NFC kartı veya etiketi ile yoklama verebilmesini güvence altına almaktadır.

Üçüncü aşama olan BLE tabanlı mesafe doğrulaması adımında, öğrencinin mobil cihazı, öğretim elemanının mobil cihazı tarafından başlatılan BLE yayınını taramaktadır. BLE sinyalinin algılanması, öğrencinin ilgili ders ortamında fiziksel olarak bulunduğunu doğrulamaya yönelik bir yakınlık doğrulama mekanizmasıdır. Bu sayede, öğrencinin sınıf dışında bulunmasına rağmen sisteme uzaktan erişerek yoklama verme olasılığı azaltılmaktadır. Android 10 ve sonraki sürümlerde BLE taraması yapılabilmesi için konum izninin etkinleştirilmiş olması gerekmektedir. Bu nedenle öğrencilerin uygulamayı ilk kez kullanırken konum iznini etkinleştirmeleri önerilmektedir. BLE sinyali başarıyla algılandığında, ilgili oturuma ait kimlik (ID) bilgisi uygulama tarafından otomatik olarak alınmakta ve doğrulama süreci bir sonraki aşamayla devam etmektedir.

Dördüncü ve son aşama olan tek kullanımlık belirteç (token) doğrulaması adımında, öğretim elemanı tarafından ders sırasında paylaşılan tek kullanımlık belirteç (token) bilgisi öğrenci tarafından uygulamaya girilmektedir. Girilen belirteç, aktif yoklama oturumuna ait belirteç bilgisiyle karşılaştırılmaktadır. Bu adım, özellikle farklı derslere ait BLE kapsama alanlarının çakışması, oturum bilgilerinin yetkisiz kişilerle paylaşılması veya yanlış yoklama oturumuna katılım sağlanması gibi riskleri azaltmak amacıyla kullanılmaktadır. Tek kullanımlık belirteç yapısı, doğrulama sürecine ek bir güvenlik katmanı kazandırmaktadır. Bu dört doğrulama adımının başarıyla tamamlanmasının ardından sistem, öğrencinin kimliğini ve ders ortamındaki fiziksel varlığını doğrulanmış kabul etmektedir. Böylece yoklama kaydı oluşturulmakta ve ilgili bilgiler veritabanına kaydedilmektedir. Doğrulama adımlarından herhangi birinin başarısız olması durumunda ise süreç sonlandırılmakta ve yoklama kaydı oluşturulmamaktadır. Bu yapı sayesinde YOKSAVAR PRO, öğrenci doğrulamasını kimlik doğrulama, kart doğrulaması, fiziksel yakınlık doğrulaması ve oturum güvenliği olmak üzere dört temel güvenlik boyutunu bütünleştiren çok katmanlı bir yoklama mekanizması sunmaktadır.



Şekil 4. Öğrenci Portalı Üzerinden Yoklama Doğrulama Süreci

3.3. Cihaz Mühürleme Mekanizması

YOKSAVAR PRO sisteminin temel güvenlik katmanlarından biri cihaz mühürleme mekanizmasıdır. Bu mekanizma, öğrencinin yalnızca kendisine kayıtlı mobil cihazı ve tanımlı NFC kartı üzerinden yoklama verebilmesini sağlamaktadır. Öğrenci ilk yoklama işlemini gerçekleştirdiğinde okul numarası, "device_info_plus" kütüphanesi aracılığıyla elde edilen cihaz kimliği (UID) ve NFC kart UID bilgisi birlikte kaydedilerek öğrenci profiliyle ilişkilendirilmektedir. İlgili kütüphane (device_info_plus), envanter yönetimi amacıyla kullanılan OCS Inventory ve GLPI Agent benzeri araçların mobil cihazlardaki karşılığı olarak değerlendirilebilir. Android işletim sisteminde ANDROID_ID, cihaz modeli, üretici bilgisi ve donanım sürümü; iOS işletim sisteminde ise "identifierForVendor" değeri ile cihaz modeli kullanılarak cihaza özgü bir kimlik oluşturulmaktadır. Oluşturulan bu kimlik, sonraki yoklama girişimlerinde öğrenci profiline kayıtlı değerle karşılaştırılmakta; farklı bir mobil cihaz veya farklı bir NFC kartı tespit edilmesi durumunda sistem yoklama işlemini reddetmektedir. Bu sayede, bir öğrencinin başka bir öğrenci adına yoklama vermesi, cihaz paylaşımı veya kart değişimi gibi güvenlik risklerinin azaltılması amaçlanmaktadır.

Mobil cihazın değiştirilmesi veya NFC kartının kaybolması gibi geçerli durumlarda öğretim elemanı ya da yetkili kullanıcı, yönetim (admin) paneli üzerinden cihaz mühürleme kaydını sıfırlayabilmektedir. Cihaz mühürleme yaklaşımı, mobil cihazlarda kimlik doğrulamanın kritik

önemini vurgulayan ve biyometrik kimlik doğrulama yöntemlerini kapsamlı biçimde inceleyen çalışmalarla (Alzubaidi ve Kalita, 2016) paralellik göstermektedir.

3.4. Bildirim Sistemi

Yoklama oturumu sonlandırıldığında Supabase Edge Function tetiklenerek ilgili derse kayıtlı öğrencilerin katılım durumları kontrol edilmektedir. Edge Function, Function-as-a-Service (FaaS) mimarisine uygun olarak yalnızca tetiklendiği anda çalıştığından bulut kaynaklarının verimli kullanılmasını sağlamaktadır (Adhoni vd., 2025). Sistem, yoklamaya katılan ve katılmayan öğrencileri otomatik olarak belirlemekte ve her öğrenciye Firebase Cloud Messaging (FCM) aracılığıyla anlık bildirim göndermektedir. FCM'nin tercih edilmesindeki temel nedenler maliyet etkinliği ve ölçeklenebilirliktir. SMS tabanlı bildirim sistemlerinde her mesaj için ayrı ücretlendirme uygulanabilmektedir. Örneğin, e-Devlet Kapısı üzerinden abonelik başvurusu ve iptali yapılabilen UYAP SMS Bilgi Sistemi'nde abonelere gönderilen her kısa mesajın (SMS), vergiler dâhil 3 TL olarak ücretlendirildiği belirtilmektedir (Adalet Bakanlığı UYAP SMS Bilgi Sistemi, 2020). Buna karşılık, Google Firebase tarafından sunulan Firebase Cloud Messaging hizmetinde Cloud Messaging kullanımından ek ücret alınmadığı ifade edilmektedir (Google Firebase, 2026). Bu nedenle YOKSAVAR PRO'da SMS yerine FCM tabanlı anlık bildirimlerin tercih edilmesi, özellikle çok sayıda öğrencinin bulunduğu yükseköğretim kurumlarında dönem boyunca oluşabilecek yoğun bildirim trafiği açısından maliyet etkin, sürdürülebilir ve ölçeklenebilir bir çözüm sunmaktadır.

Bildirim içeriği öğrencinin katılım durumuna göre değişmektedir. Yoklamaya katılan öğrenciye katılımının başarıyla kaydedildiğine ilişkin bir bildirim gönderilirken, yoklamaya katılmayan öğrenci devamsızlık durumu hakkında bilgilendirilmektedir. Devamsızlık sınırına yaklaşan veya bu sınırı aşan öğrenciler için ise ayrıca uyarı bildirimi gönderilebilmektedir. Bu yapı, öğrencilerin devamsızlık durumlarını anlık olarak takip edebilmelerine ve devam durumlarını daha etkin biçimde yönetebilmelerine olanak sağlamaktadır.

3.5. Admin Web Paneli

Yönetim (admin) web paneli, öğretim elemanlarının ve yetkili kullanıcıların veritabanıyla doğrudan etkileşime girmeden sistemi yönetebilmeleri amacıyla geliştirilmiştir. Flutter Web ile geliştirilen panel, Firebase Hosting üzerinde çalışacak şekilde tasarlanmıştır. Panel üzerinden ders yönetimi, öğrenci yönetimi, toplu veri aktarımı, muafiyet durumu güncelleme, oturum geçmişinin görüntülenmesi, devamsızlık raporlarının oluşturulması ve bildirim geçmişinin incelenmesi gibi işlemler gerçekleştirilebilmektedir. Ders yönetimi kapsamında ders kodu, ders adı, ders türü, sorumlu öğretim elemanı ve devamsızlık limiti gibi bilgiler sisteme eklenebilmekte; mevcut ders kayıtları güncellenebilmekte veya silinebilmektedir. Öğrenci yönetimi bölümünde öğrencilerin okul numarası, ad ve soyadı ile ders kayıtları yönetilebilmektedir. Kişisel verilerin korunması amacıyla panel arayüzünde ad ve soyadı bilgileri varsayılan olarak kısmen maskelenmiş biçimde sunulmakta (örneğin,

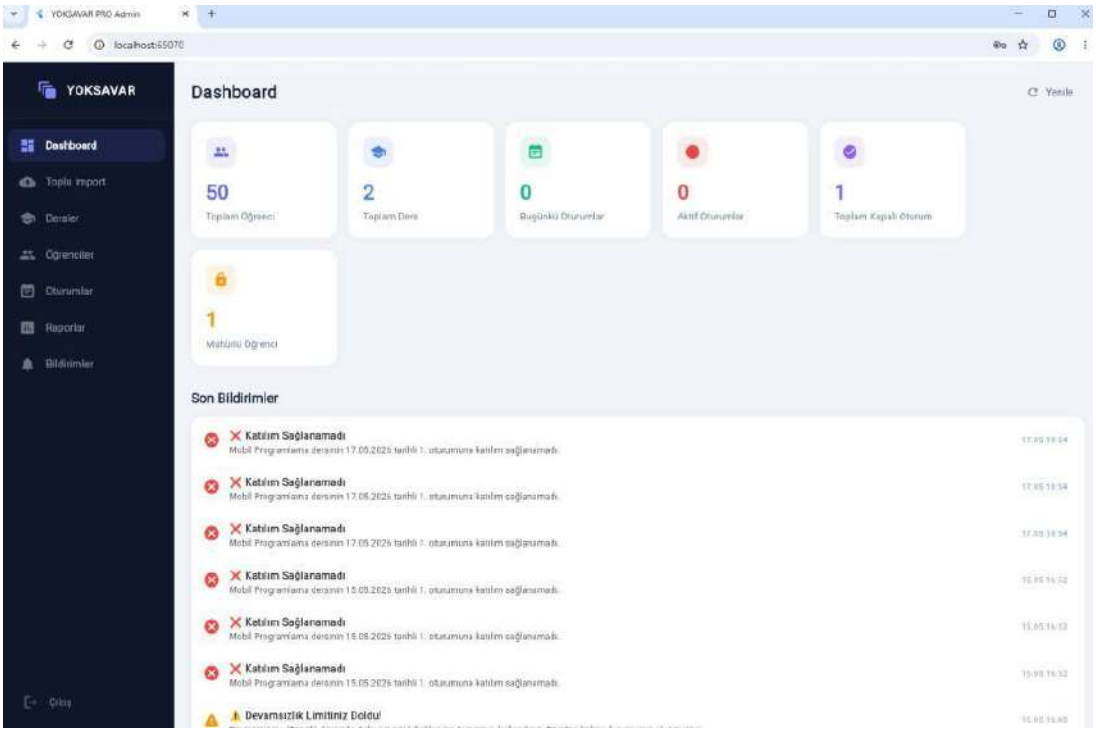
"Ahmet Y******"); raporlama amacıyla gerçekleştirilen dışa aktarma işlemlerinde ise alan bazlı erişim yetkilendirmesi uygulanmaktadır. Bu yaklaşım, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun veri minimizasyonu ilkesiyle uyumludur. Öğrencilere ait cihaz mühürleme bilgileri ve NFC kart UID kayıtları da bu panel üzerinden görüntülenebilmekte ve yönetilebilmektedir.

Toplu veri aktarımı özelliği sayesinde öğrenci listeleri Comma-Separated Values (CSV) formatında sisteme aktarılabilmektedir. CSV formatı, öğrenci bilgilerinin tablo yapısında hazırlanarak sisteme toplu olarak yüklenmesini kolaylaştırmaktadır. Veri aktarımı sırasında öğrenci kayıtları, ders eşleştirmeleri ve NFC kart bilgileri sistem tarafından otomatik olarak işlenmektedir. Hatalı veya eksik kayıtlar kullanıcıya raporlanarak veri aktarım sürecinin daha güvenilir ve kontrollü biçimde yürütülmesi sağlanmaktadır. Bunun yanında öğrenci listeleri, devamsızlık kayıtları ve yoklama oturumlarına ilişkin veriler de CSV formatında dışa aktarılabilmektedir. NFC kart altyapısı açısından, kurumsal akıllı kart sistemine sahip öğrenciler için mevcut üniversite kartlarının kullanılması öngörülmektedir. Bu çalışmanın uygulandığı üniversitede SOFRA sistemi, öğrenci işlemlerinde kullanılan kurumsal servislerden biri olduğundan NFC altyapısı olarak mevcut kurumsal kart yapısı esas alınmıştır (Bilecik Şeyh Edebali Üniversitesi, 2024).

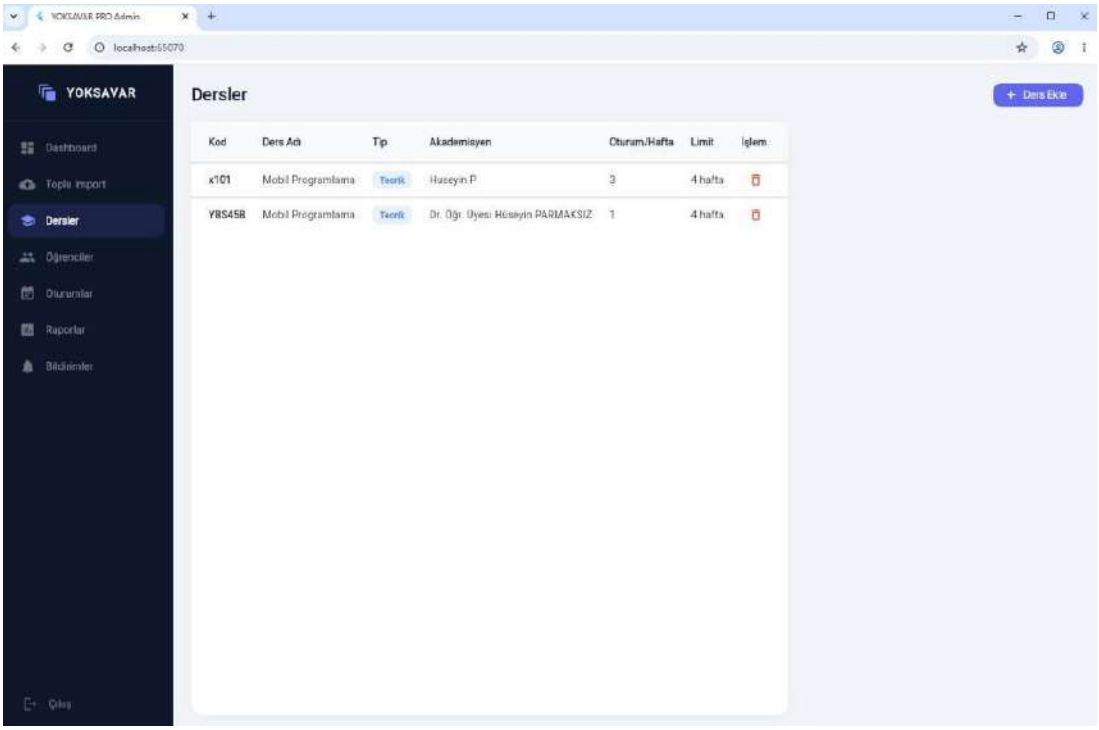
Kurumsal kart altyapısının yeterli olmadığı veya test ortamlarında harici kart okuma ve yazma gereksiniminin ortaya çıktığı durumlarda Arduino uyumlu NFC/RFID okuyucu modülleri alternatif çözüm olarak değerlendirilebilmektedir. Arduino Store'da yer alan NFC/RFID Reader with Two Transponders ürünü bu amaçla kullanılabilmekte; RC522 ve PN532 modüllerinin Arduino Uno, Arduino Nano, Arduino Mega 2560 ve Raspberry Pi gibi geliştirme kartlarıyla uyumlu çalıştığı bilinmektedir (Arduino, 2026; Adafruit, 2013). Nitekim literatürde de benzer eğitim ortamlarında geliştirilen elektronik yoklama sistemlerinde PN532 modülünün tercih edildiği görülmektedir (Du vd., 2025; Szolga vd., 2025). Bununla birlikte, söz konusu modüller YOKSAVAR PRO'nun temel çalışma mimarisinin zorunlu bir bileşeni değildir. Bu modüller; NFC kartlarının tanımlanması, test edilmesi ve alternatif okuma-yazma senaryolarının desteklenmesi amacıyla kullanılan yardımcı donanımlar olarak değerlendirilmektedir.

Özellikle iOS platformunda NFC kartına yazma işlemleri için tarafımızca geliştirilen yardımcı uygulamadan yararlanılmıştır. Bu sayede sistem, mobil cihaz üzerinden NFC kartlarının tanımlanması, öğrenci bilgileriyle eşleştirilmesi ve yoklama sürecinde UID doğrulamasının gerçekleştirilmesini daha güvenli ve kontrollü biçimde yürütecek şekilde tasarlanmıştır.

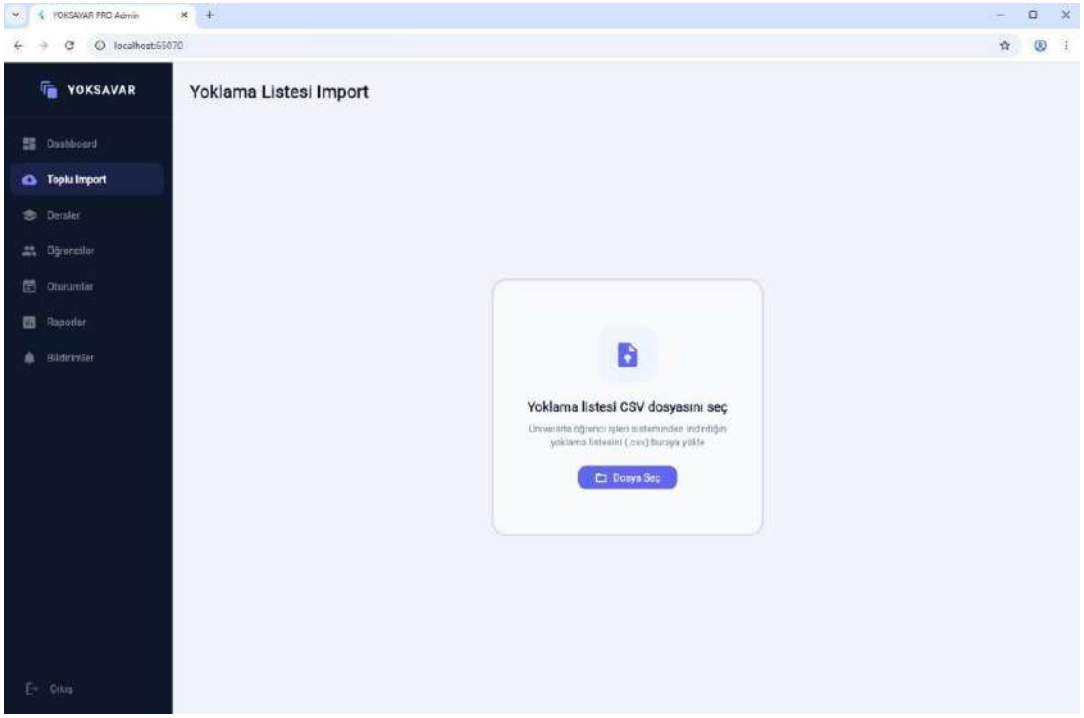
Muafiyet durumu güncelleme özelliği sayesinde belirli öğrenciler devamsızlık hesaplamalarından muaf tutulabilmektedir. Bu özellik, sağlık raporu veya geçerli mazeret gibi durumların sistem üzerinden etkin biçimde yönetilebilmesine olanak sağlamaktadır.



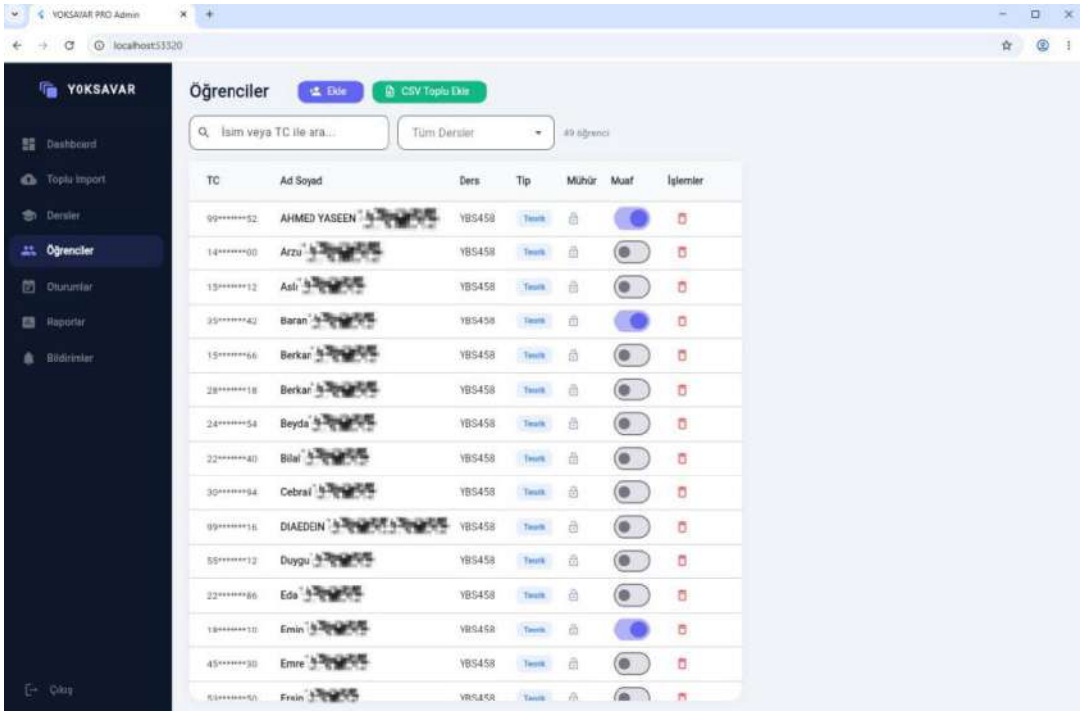
Şekil 5. Admin Web Paneli



Şekil 6. Admin Web Paneli: Ders Yönetimi



Şekil 7. Admin Web Paneli: Toplu CSV İçe Aktarma ve Dışa Aktarma Ekranı



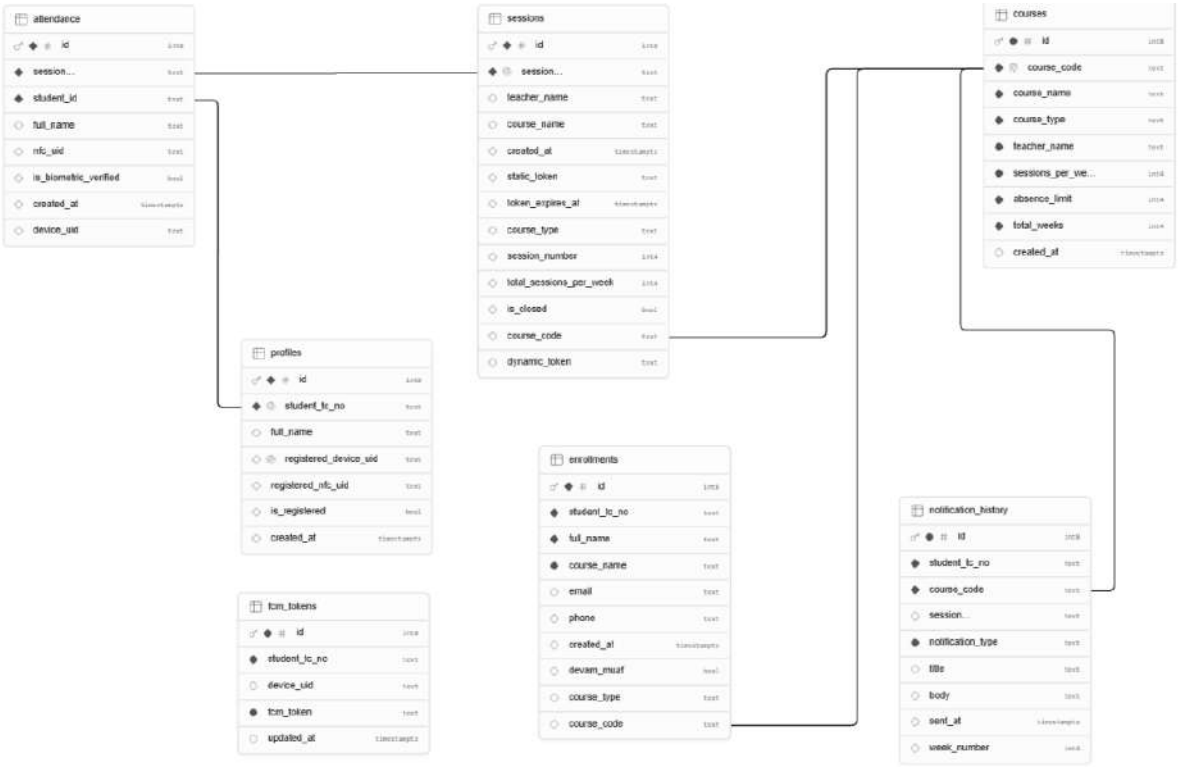
Şekil 8. Admin Web Paneli: Muafiyet Durumu Güncelleme ve Devamsızlık Raporları Ekranı

3.6. Veritabanı Mimarisi

YOKSAVAR PRO sistemi, Supabase PostgreSQL veritabanı üzerinde yapılandırılmıştır. Veritabanı; ders tanımları, öğrenci-ders eşleştirmeleri, yoklama oturumları, yoklama kayıtları, cihaz ve NFC mühürleme bilgileri, bildirim belirteçleri (token) ile bildirim geçmişi gibi temel veri yapılarını içermektedir. Sistemde kullanılan başlıca tablolar courses, enrollments, sessions, attendance, profiles,

fcm_tokens ve notification_history tablolarıdır. courses tablosunda ders bilgileri, enrollments tablosunda öğrenci-ders ilişkileri, sessions tablosunda oluşturulan yoklama oturumları, attendance tablosunda yoklama kayıtları, profiles tablosunda öğrencilere ait cihaz ve NFC mühürleme bilgileri, fcm_tokens tablosunda bildirim gönderimi için gerekli cihaz belirteçleri (token) ve notification_history tablosunda gönderilen bildirim geçmişi saklanmaktadır.

Tablolar arasındaki ilişkiler temel olarak course_code ve student_school_no alanları üzerinden kurulmuştur. PostgreSQL'in Row Level Security (RLS) özelliği sayesinde her kullanıcı yalnızca erişim yetkisine sahip olduğu kayıtlara ulaşabilmektedir. Böylece çok kiracılı (multi-tenant) bir mimarinin temel altyapısı da oluşturulmaktadır (Supabase, 2022). Bu tasarım sayesinde öğrencilerin ders kayıtları, yoklama oturumları, katılım durumları, cihaz mühürleme bilgileri ve bildirim geçmişleri ilişkisel veritabanı yapısı içerisinde bütüncül olarak yönetilebilmekte ve izlenebilmektedir.



Şekil 9. Veritabanı Mimarisi

Kaynak:Yazarlar tarafından Supabase Schema Visualizer aracılığıyla alınmıştır.

4. BULGULAR

Bu bölümde, YOKSAVAR PRO sisteminin 1 öğretim elemanı ve 9 öğrenci olmak üzere toplam 10 farklı mobil cihaz üzerinde gerçekleştirilen testlerden elde edilen bulgular sunulmaktadır. Öğretim elemanına ait mobil cihaz (Xiaomi Redmi Note 9 Pro), hem öğretim elemanı rolünde (BLE yayınının başlatılması ve yoklama oturumunun yönetilmesi) hem de öğrenci rolünde (BLE sinyalinin algılanması, biyometrik kimlik doğrulama, NFC kart doğrulaması ve tek kullanımlık belirteç [token]

doğrulaması) farklı oturumlarda test edilmiştir. Her öğrenci cihazında iki yoklama oturumu gerçekleştirilmiş ve toplam 20 yoklama oturumu tamamlanmıştır. Test ortamında kullanılan mobil cihazların teknik özellikleri AIDA64 (sürüm 2.20) uygulaması ile, BLE ölçümleri nRF Connect uygulaması ile, Android cihaz kimlik bilgileri ise Device ID uygulaması kullanılarak belirlenmiştir. Testlerde kullanılan mobil cihazların teknik özellikleri Tablo 2'de sunulmaktadır.

Tablo 2 Test Ortamında Kullanılan Mobil Cihazların Teknik Özellikleri

Cihaz Modeli	Rolü	Android Sürümü	Bluetooth Sürümü	SoC Modeli	Bluetooth Adresi	NFC Desteği
Xiaomi Redmi Note 11S	Öğrenci	11	5.0	MediaTek Helio G96	44:71:47:00:00:**	Yok
Xiaomi Redmi Note 9 Pro	Öğretim Üyesi	12	5.0	Snapdragon 720G	98:f6:21:32:78:**	Var
Xiaomi Redmi 13C 4G	Öğrenci	14	5.3	MediaTek Helio G85	38:c6:bd:de:f1:**	Yok
Realme C55	Öğrenci	15	5.2	MediaTek Helio G88	b8:8f:27:fa:86:**	Var
Samsung Galaxy A35	Öğrenci	16	5.3	Exynos 1380	c8:51:42:e4:dd:**	Var
Samsung Galaxy A56	Öğrenci	16	5.4	Exynos 1580	54:dd:4f:04:eb:**	Var
Samsung Galaxy A55	Öğrenci	16	5.3	Exynos 1480	08:a5:df:f7:74:**	Var
Xiaomi Redmi Note 11S(2)	Öğrenci	13	5.0	MediaTek Helio G96	e4:84:d3:73:8b:**	Yok
Xiaomi Redmi Note 10 Pro	Öğrenci	13	5.0	Snapdragon 732G	a4:55:90:19:28:**	Var
Xiaomi Redmi Note 12	Öğrenci	13	5.1	Snapdragon 685	44:71:47:00:00:**	Var

Bluetooth adreslerinin ilk üç okteti (OUI – Organizationally Unique Identifier) IEEE tarafından atanmakta olup cihaz üreticisini tanımlamaktadır. Bu kapsamda 44:71:47, 38:C6:BD, E4:84:D3 ve A4:55:90 ön ekleri Xiaomi cihazlarını; 98:F6:21, C8:51:42, 54:DD:4F ve 08:A5:DF ön ekleri Samsung cihazlarını; B8:8F:27 ön eki ise Realme cihazlarını göstermektedir. Tabloda yer alan Bluetooth adresleri, test ortamında kullanılan cihazların donanım çeşitliliğini ve farklı üreticilere ait mobil cihazların sistemle uyumluluğunu göstermek amacıyla sunulmuştur. Cihaz mühürleme mekanizması doğrudan Bluetooth adresine dayanmamakta; "device_info_plus" kütüphanesi aracılığıyla elde edilen ANDROID_ID, cihaz modeli, üretici bilgisi ve donanım sürümü gibi daha kararlı ve kalıcı tanımlayıcıları kullanmaktadır. Bu yaklaşım, Bluetooth adresinde meydana gelebilecek değişikliklerden veya işletim sisteminin erişim kısıtlamalarından etkilenmemektedir.

NFC donanımı bulunmayan mobil cihazlarda ise sistem, kullanıcıların UID bilgisini manuel olarak girmesine olanak tanımaktadır. Girilen UID bilgisi "shared_preferences" kütüphanesi kullanılarak cihazda kalıcı olarak saklanmakta ve sonraki yoklama oturumlarında otomatik doldurma özelliği sayesinde ilgili alanlara otomatik olarak yerleştirilmektedir. Xiaomi Redmi Note 9 Pro (*), hem öğretim elemanı hem de öğrenci rolünde test edilmiştir.

4.1. Doğrulama Katmanlarının Başarı Oranları

Öğrenci doğrulama sürecindeki dört güvenlik katmanı (biyometrik kimlik doğrulama, NFC kart doğrulaması, BLE tabanlı mesafe doğrulaması ve tek kullanımlık belirteç [token] doğrulaması), 10 farklı öğrenci cihazında her cihaz için iki yoklama oturumu gerçekleştirilerek toplam 20 oturumda ayrı ayrı değerlendirilmiştir. Biyometrik kimlik doğrulama adımında 20 oturumun tamamı başarıyla sonuçlanmış ve %100 başarı oranı elde edilmiştir. NFC kart doğrulaması da %100 başarı oranı ile tamamlanmıştır. NFC donanımı bulunmayan üç mobil cihazda gerçekleştirilen altı oturumda ise doğrulama, manuel UID girişi ile başarıyla gerçekleştirilmiştir. Tek kullanımlık belirteç (token) doğrulaması aşamasında da tüm öğrenciler doğru belirteç bilgisini girmiş ve %100 başarı oranına ulaşılmıştır. BLE tabanlı mesafe doğrulaması aşamasında ise 20 oturumun 19'u başarıyla tamamlanmış, yalnızca bir oturumda doğrulama başarısız olmuştur. Bu başarısızlık, öğrenci cihazında Android işletim sistemine ait konum izninin etkinleştirilmemiş olmasından kaynaklanmıştır. Android 10 ve sonraki sürümlerde BLE taramasının gerçekleştirilebilmesi için konum izninin etkinleştirilmiş olması zorunludur. Dolayısıyla bu durum sistemden kaynaklanan bir hata olmayıp, BLE tabanlı yakınlık doğrulamasının çalışabilmesi için yerine getirilmesi gereken işletim sistemi koşullarından biridir. Konum izni etkinleştirildikten sonra aynı cihazla gerçekleştirilen tekrar testinde BLE sinyali başarıyla algılanmıştır. Dört doğrulama katmanının tamamının başarıyla tamamlandığı oturumların oranı %95 olarak hesaplanmıştır.

4.2. Doğrulama ve Bildirim Süreleri

Cihaz bazında ölçülen toplam doğrulama süresi (biyometrik, NFC, BLE ve token adımlarının tamamı), BLE algılama süresi ve bildirim gecikmesi Tablo 3’te sunulmaktadır. Öğretmen cihazı (Xiaomi Redmi Note 9 Pro), öğrenci rolünde de ayrı test oturumlarında kullanılmış ve bu oturumlarda da bildirim alabilmiştir.

Tablo 3 Yoklama Süreci Aşamalarının Analizi

Cihaz Modeli	Rolü	Toplam Doğrulama Süresi	BLE Algılama Süresi	Bildirim Gecikmesi
Xiaomi Redmi Note 11S	Öğrenci	28,32	1,55	20,08
Xiaomi Redmi Note 9 Pro	Öğrenci	20,56	1,01	4,40
Realme C55	Öğrenci	30,85	1,57	22,54
Samsung Galaxy A35	Öğrenci	26,86	1,25	26,86
Samsung Galaxy A56	Öğrenci	31,34	1,65	31,34
Samsung Galaxy A55	Öğrenci	29,69	1,58	29,69
Xiaomi Redmi Note 11S (2)	Öğrenci	27,58	1,27	27,58
Xiaomi Redmi Note 10 Pro	Öğrenci	26,83	1,42	26,83
Xiaomi Redmi Note 12	Öğrenci	27,50	1,48	22,50
Xiaomi Redmi 13C 4G	Öğrenci	31,20	1,60	23,10

Not: Öğretim üyesi cihazı (Xiaomi Redmi Note 9 Pro), öğrenci rolünde de ayrı test oturumlarında kullanılmış olup, tabloda "Öğrenci" rolü altında gösterilmektedir.

Toplam doğrulama süresi cihazlar arasında 26,83 ile 31,34 saniye arasında değişmektedir. NFC kartının manuel olarak tanımlanmasını gerektiren cihazlarda (Xiaomi Redmi Note 11S, Xiaomi Redmi Note 11S (2) ve Xiaomi Redmi 13C 4G) toplam doğrulama süresinin 27,58–31,20 saniye aralığında olduğu, NFC kartını doğrudan okuyabilen cihazlarda ise bu sürenin 26,83–29,69 saniye aralığında kaldığı gözlenmiştir. En kısa toplam doğrulama süresi Xiaomi Redmi Note 10 Pro'da 26,83 saniye, en uzun doğrulama süresi ise Samsung Galaxy A56'da 31,34 saniye olarak ölçülmüştür.

BLE tabanlı mesafe doğrulaması kapsamında BLE sinyalinin algılanma süresi tüm cihazlarda ortalama 1,45 saniye olarak ölçülmüştür. Bu süre, öğretim elemanının mobil cihazında BLE yayınının başlatılması ile öğrenci cihazının bu yayını algılaması arasında geçen süreyi ifade etmektedir. En kısa BLE algılama süresi 1,25 saniye ile Samsung Galaxy A35'te, en uzun süre ise 1,65 saniye ile Samsung Galaxy A56'da ölçülmüştür. Bildirim gecikmesi ölçümlerinde öğretim elemanının mobil cihazı ile öğrenci cihazları arasında belirgin bir farklılık gözlenmiştir. Öğretim elemanına ait mobil cihazda ortalama bildirim gecikmesi 4,40 saniye (SS = 0,03) olarak ölçülürken, öğrenci cihazlarında bu süre ortalama 25,61 saniye (SS = 4,41) olarak belirlenmiştir. Bu farklılığın, öğretim elemanına ait cihazın geliştirme sürecinde en yoğun biçimde test edilmesi ve optimize edilmesinden kaynaklanmış olabileceği değerlendirilmektedir. Ayrıca öğretim elemanı cihazındaki bildirimlerin doğrudan FCM üzerinden iletilmesine karşılık, öğrenci cihazlarında bildirimlerin önce Supabase Edge Function tarafından işlenmesi, katılım durumunun değerlendirilmesi ve ardından FCM aracılığıyla gönderilmesi de gecikme süresini etkileyen etkenlerden biri olarak değerlendirilmektedir. Öğretim elemanına ait mobil cihaz öğrenci rolünde test edildiğinde de, diğer öğrenci cihazlarına kıyasla daha düşük bildirim gecikmesi gözlenmiştir.

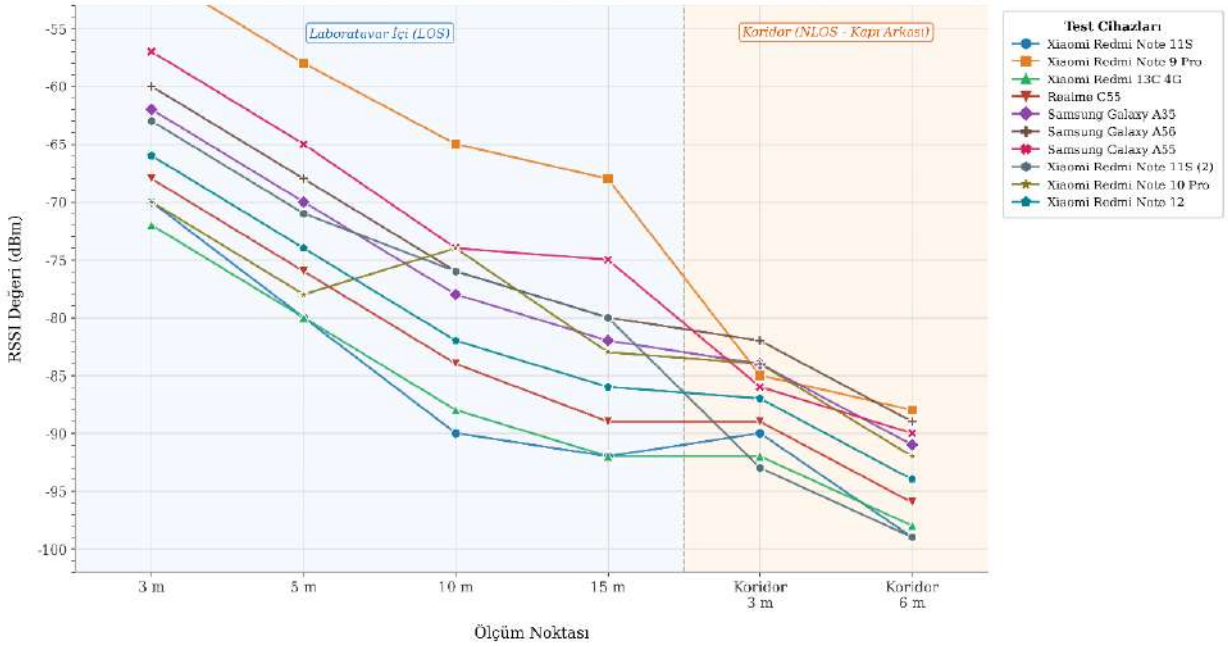
4.3. Cihaz Mühürleme Performansı

Cihaz mühürleme mekanizması, iki farklı senaryoda toplam 40 deneme ile test edilmiştir. Birinci senaryoda, kayıtlı olmayan bir cihaz veya farklı bir NFC kart ile yoklama verilmeye çalışılmış ve 20 denemenin tamamında sistem bu girişimleri başarıyla engellemiştir. Kayıtlı cihazda farklı bir NFC kart kullanıldığında veya kayıtlı NFC kart farklı bir cihazda kullanıldığında sistem, eşleşmeyen UID bilgisi nedeniyle yoklama işlemini reddetmiştir.

İkinci senaryoda, admin paneli üzerinden öğrencinin cihaz mühürleme kaydı sıfırlanmış ve ardından öğrencinin yeni cihazıyla yoklama vermesi denenmiştir. 20 denemenin tamamında sistem, yeni cihaz UID’sini ve NFC kart UID’sini başarıyla profile kaydederek yeniden mühürleme işlemini gerçekleştirmiştir. Her iki senaryoda da %100 başarı oranı elde edilmiştir.

4.4. BLE Sinyal Gücü ve Menzil Değerlendirmesi

BLE sinyal gücü (RSSI), doğru görüş hattı (LOS) ve doğru görüş hattı olmayan (NLOS) ortamlarda farklı mesafelerde nRF Connect uygulaması ile ölçülmüştür. RSSI değerleri desibel-milliwatt (dBm) cinsinden ifade edilmekte olup, daha negatif değerler daha zayıf sinyal seviyesini göstermektedir. Elde edilen ölçüm sonuçlarına göre oluşturulan grafik Şekil 10'da sunulmaktadır.



Şekil 10. Test Edilen Android Cihazlarda BLE RSSI Değerlerinin Ölçüm Noktasına Göre Değişimi

Şekil 10 incelendiğinde, tüm cihazlarda laboratuvar ortamında (LOS) 3 metre mesafede RSSI değerlerinin yaklaşık -57 dBm civarında olduğu, 5 metrede -65 dBm'ye, 10 ve 15 metrede ise -72 dBm seviyesine düştüğü görülmektedir. 10 metre ile 15 metre arasında RSSI değerlerinde belirgin bir fark oluşmaması, bu mesafelerde BLE sinyalinin sönümlenme eğrisinin yataylaşmaya başladığını ve sinyalin kararlı ancak zayıf seviyede kaldığını göstermektedir. Koridor ortamında (NLOS) ise 3 metre mesafede ortalama RSSI değerinin yaklaşık -70 dBm, 6 metrede ise -72 dBm olduğu gözlenmiştir. LOS ortam ile karşılaştırıldığında, NLOS ortamda aynı mesafelerde yaklaşık 10–13 dBm ek sinyal zayıflaması meydana gelmektedir. Bu durum, fiziksel engellerin (duvarlar, kapılar) BLE sinyali üzerindeki zayıflatıcı etkisini açıkça ortaya koymaktadır. Cihazlar arasında RSSI değerlerinde küçük farklılıklar gözlenmekle birlikte, genel eğilim tüm cihazlarda benzerdir. Bu bulgular, sistemin 10 metreye kadar olan sınıf içi mesafelerde (LOS) güvenilir BLE bağlantısı sağlayabildiğini, NLOS ortamlarda ise sinyal kalitesinin belirgin şekilde düştüğünü göstermektedir. BLE sinyalinin iç mekândaki davranışı, özellikle parmak izi tabanlı konumlandırma çalışmalarında (Faragher & Harle, 2015) ayrıntılı olarak incelenmiştir. Bu çalışmada elde edilen RSSI değerlerinin mesafeyle değişim eğilimi, söz konusu literatürle tutarlılık göstermekte olup, fiziksel engellerin sinyal üzerindeki zayıflatıcı etkisi beklenen bir sonuç olarak değerlendirilmektedir.

4.5. Karşılaşılan Sorunlar ve Çözümleri

Testler sırasında NFC ile ilgili iki temel durum gözlenmiştir. İlk olarak, NFC donanımı bulunmayan üç cihazda (Xiaomi Redmi Note 11S, ikinci Xiaomi Redmi Note 11S ve Xiaomi Redmi 13C 4G) UID bilgisinin manuel olarak girilmesi gerekmiştir. Bu cihazları kullanan öğrenciler, UID bilgilerini NFC özellikli bir mobil cihaz aracılığıyla kartlarını okutarak veya kurumsal kart bilgilerinden temin edebilmektedir. Girilen UID bilgileri, "shared_preferences" kütüphanesi kullanılarak cihazda kalıcı olarak saklanmakta ve sonraki yoklama oturumlarında otomatik doldurma özelliği sayesinde ilgili alanlara otomatik olarak yerleştirilmektedir. Böylece öğrencilerin her yoklama oturumunda UID bilgisini yeniden girmesine gerek kalmamakta ve manuel veri girişinden kaynaklanan iş yükü azaltılmaktadır. İkinci olarak, Realme C55 cihazında gerçekleştirilen iki oturumda NFC okuma işlemi, kartın temassız okuma alanına ilk denemede doğru şekilde temas ettirilmemesi nedeniyle başarısız olmuş; ikinci denemede ise başarıyla tamamlanmıştır. Bu durum, sistemden değil kullanıcı kaynaklı bir kullanım hatasından kaynaklanmaktadır. Bunun dışında test edilen diğer tüm cihazlarda NFC doğrulamasına ilişkin herhangi bir sorunla karşılaşılmamıştır. Konum izninin etkinleştirilmesi, sistemden kaynaklanan bir hata değil, Android işletim sisteminde BLE taramasının gerçekleştirilebilmesi için yerine getirilmesi gereken bir kullanıcı ön koşuludur. Bu nedenle söz konusu durum, bu bölümde bir sistem sorunu olarak değerlendirilmemiştir. İlgili ön koşul, Bölüm 3.2'de (Öğrenci Doğrulama Süreci) ayrıntılı olarak açıklanmıştır.

5. SONUÇ VE ÖNERİLER

Bu çalışmada geliştirilen YOKSAVAR PRO sistemi, üniversitelerdeki yoklama süreçlerini dijitalleştirmeyi ve sahte yoklama girişimlerini azaltmayı hedefleyen çok katmanlı bir mobil çözüm sunmaktadır. Elde edilen bulgular, sistemin dört doğrulama katmanını (biyometrik, NFC, BLE, token) başarıyla çalıştırdığını ve tüm katmanları tamamlayan oturum oranının %95 olduğunu göstermiştir. Bu başarı oranı, literatürdeki tek katmanlı sistemlerin güvenlik zafiyetlerine karşı önemli bir iyileştirme sağlamaktadır. Cihaz mühürleme mekanizmasının proxy girişimlerini %100 oranında engellemesi, bu çok katmanlı yaklaşımın pratikteki etkinliğini doğrulamaktadır.

Kim vd. (2018) tarafından yapılan çalışma, BLE beacon tabanlı elektronik yoklama sistemlerinin sinyal taklidi saldırılarına karşı kırılgan olabileceğini göstermiştir. Bu bağlamda YOKSAVAR PRO, BLE sinyalini tek başına yeterli görmeyerek NFC kart doğrulama, biyometrik kimlik doğrulama, tek kullanımlık token ve cihaz mühürleme katmanlarıyla desteklemiştir. Literatürdeki mevcut sistemler genellikle tek bir teknolojiye odaklanmakta ve sınırlı sayıda doğrulama katmanı sunmaktadır (Alcantara vd., 2022; Chiang vd., 2022; Jain, 2025; Munivrana vd., 2025; Nagarajan vd., 2025; Shaikh vd., 2026). YOKSAVAR PRO, fiziksel yakınlık, kart doğrulama, yerel biyometrik onay, oturum bazlı token, cihaz mühürleme ve yoklama sonrası bildirim adımlarını bütünleşik bir akış içinde sunarak bu eksiklikleri gidermeyi amaçlamaktadır.

Sistemin ek donanım gerektirmemesi, RFID okuyucu, NFC okuyucu, mikrodenetleyici veya BLE beacon gibi bileşenlere ihtiyaç duyan çözümlere kıyasla (Sezdi ve Tüysüz, 2018; Özcan vd., 2018; Du vd., 2025; Üçgün vd., 2018) önemli bir maliyet avantajı sunmaktadır. Mevcut mobil cihazlar üzerinden çalışabilmesi, özellikle sınıf sayısı fazla olan kurumlarda kurulum, bakım ve ölçeklendirme maliyetlerini azaltmaktadır. Bildirim mekanizmasında Firebase Cloud Messaging (FCM) kullanılması, SMS tabanlı sistemlere göre maliyet etkin ve ölçeklenebilir bir çözüm sunmaktadır (Google Firebase, 2026; Adalet Bakanlığı UYAP SMS Bilgi Sistemi, 2020). Ayrıca, sistemin güvenlik değerlendirmesi kapsamında MobSF ile yapılan statik analiz, uygulamanın 100 üzerinden 78 puan aldığını ve düşük risk (LOW RISK) düzeyinde değerlendirildiğini göstermiştir (Mobile Security Framework [MobSF], 2026). Rapor, uygulamanın Grade A seviyesinde bir güvenlik notu aldığını ve herhangi bir yüksek riskli güvenlik açığı barındırmadığını ortaya koymuştur.

Gerçek sınıf ortamında yapılan 20 oturumluk testler, sistemin %95 başarı oranıyla çalıştığını, BLE algılama süresinin ortalama 1,45 saniye olduğunu ve cihaz mühürlemenin yetkisiz girişimleri %100 engellediğini ortaya koymuştur. Bu bulgular, geliştirilen sistemin geleneksel yoklama yöntemlerinde karşılaşılan zaman kaybı, veri güvenilirliği ve vekâleten yoklama gibi problemlere karşı uygulanabilir bir dijital çözüm sunduğunu göstermektedir. Çalışma, SDG-4 ve SDG-9 hedeflerini destekleyen bir Education 4.0 uygulaması olarak dijital yoklama sistemlerinin güvenlik, sürdürülebilirlik ve uygulanabilirlik boyutlarına katkı sağlamaktadır (United Nations, 2015).

Bununla birlikte, bu çalışma kapsamında gerçekleştirilen testler, tek bir üniversitede ve sınırlı sayıda cihaz (10 Android modeli) üzerinde yürütülmüştür. Testler orta ve üst segment Android cihazlara odaklanmış olup, düşük donanımlı veya eski Android sürümlerine sahip cihazlarda sistemin performansı ayrıca değerlendirilmemiştir. iOS işletim sistemine sahip cihazlarda test yapılamamış olması, çapraz platform performansına ilişkin bulguları sınırlamaktadır. BLE sinyal ölçümleri belirli bir sınıf ve koridor ortamında yapılmış olup, farklı fiziksel koşullarda (yoğun kalabalık, farklı duvar yapıları) sinyal davranışı değişebilir. Kullanıcı deneyimi yalnızca işlevsel testlerle değerlendirilmiş, standart bir kullanıcı kabul testi (ör. SUS) uygulanmamıştır. NFC desteği olmayan cihazlarda manuel UID girişi zorunlu tutulmuş, bu durum kullanıcı etkileşimini artırmış ve doğrulama süresini uzatmıştır.

Gelecek çalışmalarda, sistemin kullanıcılar tarafından benimsenme düzeyinin, Teknoloji Kabul Modeli (Technology Acceptance Model) çerçevesinde (Scherer vd., 2019) değerlendirilmesi önerilmektedir. Bu sayede, YOKSAVAR PRO'nun teknik başarısının yanı sıra, kullanıcı deneyimi ve kurumsal kabulüne ilişkin daha bütüncül bir analiz sunulabilecektir. Ayrıca, sistemin daha geniş öğrenci grupları ve farklı derslik türlerinde pilot uygulamalarla test edilmesi; iOS cihazlarda performansının değerlendirilmesi ve kullanıcı deneyiminin Sistem Kullanılabilirlik Ölçeği gibi standart ölçeklerle analiz edilmesi önerilmektedir. Güvenliği artırmak amacıyla, belirli aralıklarla yenilenen ve kısa geçerlilik süresine sahip dinamik token mekanizması geliştirilebilir. İnternet bağlantısının kesintili olduğu ortamlar için, yoklama verilerinin yerelde güvenli biçimde saklanıp daha

sonra senkronize edilmesini sağlayan çevrimdışı çalışma modu tasarlanabilir. Sınıf içi fiziksel varlığın desteklenmesi amacıyla, KVKK uyumlu ve anonimleştirilmiş Wi-Fi tabanlı ek bir doğrulama katmanı değerlendirilebilir. iOS platformuna özel olarak Core NFC, Face ID/Touch ID entegrasyonu ve TestFlight dağıtım süreçleri iyileştirilebilir. Sistemin farklı üniversitelerde kullanılabilmesi için çoklu kurum (multi-tenant) desteği, kurumsal rol tabanlı yetkilendirme ve veri izolasyonu özelliklerinin geliştirilmesi planlanmaktadır. Ayrıca, root/jailbreak yetkisi verilmiş cihazlarda sistem dosyalarına müdahale edilerek cihaz kimlik bilgilerinin taklit edilmesi veya NFC emülasyonu gibi suistimallerin önlenmesi için sunucu tarafında çalışan bir risk analiz modülü ve cihaz bütünlük kontrolü mekanizması geliştirilmesi öngörülmektedir. Bu kapsamda Google'ın SafetyNet Attestation veya Play Integrity API gibi servislerinin entegrasyonu değerlendirilecektir.

Sonuç olarak YOKSAVAR PRO, üniversitelerdeki yoklama süreçlerine güvenli, denetlenebilir, mobil cihazlara dayalı ve maliyet etkin bir yaklaşım sunmaktadır. Literatürdeki mevcut çözümlerle karşılaştırıldığında sistemin en güçlü yönü, farklı doğrulama katmanlarını tek bir yoklama akışı içinde birleştirmesi ve bunu ek sınıf donanımı gerektirmeden gerçekleştirebilmesidir.

KAYNAKÇA

Adalet Bakanlığı UYAP SMS Bilgi Sistemi. (2020). *Ücretlendirme*. Erişim tarihi: 20 Mayıs 2026, https://sms.uyap.gov.tr/ucretlendirme

Adafruit. (2013, 14 Ağustos). *Adafruit shield compatibility guide*. Erişim tarihi: 20 Mayıs 2026, https://learn.adafruit.com/adafruit-shield-compatibility

Adhoni, Z. A., & Narayan, D. L. (2025). Improving the interoperability of a Function-as-a-Service platform using an orchestration framework with a cloud-agnostic approach. *ETRI Journal, 47*(2), 312–325. https://doi.org/10.4218/etrij.2023-0443

Alcantara, L. G., Balagtas, A. M. T., Britania, T., Garibay, S. K., Uyvico, J. W., & Tiglao, N. M. (2022). Implementation and performance analysis of smart attendance checking using BLE-based communications. In H. Jin, C. Liu, A. S. K. Pathan, Z. M. Fadlullah, & S. Choudhury (Eds.), *Cognitive radio oriented wireless networks and wireless internet* (pp. 253–268). Springer. https://doi.org/10.1007/978-3-030-98002-3_19

Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials, 18*(3), 1998–2026. https://doi.org/10.1109/COMST.2016.2537748

Apple Inc. (2014, 23 Ekim). *TestFlight beta testing for everyone*. Apple Developer News. Erişim tarihi: 20 Mayıs 2026, https://developer.apple.com/news/?id=10232014a

Apple Inc. (2017). *Introducing Core NFC*. Apple Developer Videos. Erişim tarihi: 20 Mayıs 2026, https://developer.apple.com/videos/play/wwdc2017/718/

Arduino. (2026). *NFC/RFID reader with two transponders*. Erişim tarihi: 20 Mayıs 2026, https://store.arduino.cc/products/nfc-rfid-reader-with-two-transponders

Bilecik Şeyh Edebali Üniversitesi. (2024, 23 Temmuz). *Kurumsal öğrenci e-posta duyurusu*. Erişim tarihi: 20 Mayıs 2026, https://www.bilecik.edu.tr/lisansustu/icerik/Kurumsal_ogrenci_E_Posta_Duyurusu

Chiang, T.-W., Yang, C.-Y., Chiou, G.-J., Lin, F.-Y. S., Lin, Y.-N., Shen, V. R., Juang, T. T.-Y., & Lin, C.-Y. (2022). Development and evaluation of an attendance tracking system using smartphones with GPS and NFC. *Applied Artificial Intelligence, 36*(1), 2083796. https://doi.org/10.1080/08839514.2022.2083796

Du, J. M. H., Gervacio, P. M. D., Santisteban, K. A., Solacito, P. L. S., & Balais, M. A. (2025). A secure and automated student attendance tracking system utilizing NFC technologies for junior high school students at the UST. *IET Conference Proceedings*. https://doi.org/10.1049/icp.2025.0229

Faragher, R., & Harle, R. (2015). Location fingerprinting with Bluetooth Low Energy beacons. *IEEE Journal on Selected Areas in Communications, 33*(11), 2418–2428. https://doi.org/10.1109/JSAC.2015.2430281

Flutter Community. (2024). *device_info_plus*. Erişim tarihi: 20 Mayıs 2026, https://pub.dev/packages/device_info_plus

Google Firebase. (2026, 19 Mayıs). *Firebase Cloud Messaging*. Erişim tarihi: 20 Mayıs 2026, https://firebase.google.com/docs/cloud-messaging

Google Firebase. (2026, 19 Mayıs). *Firebase Hosting*. Erişim tarihi: 20 Mayıs 2026, https://firebase.google.com/docs/hosting

Google LLC. (2023). *Flutter — Build apps for any screen*. Erişim tarihi: 20 Mayıs 2026, https://flutter.dev/

Jain, A. (2025). A BLE-based smart attendance system for scalable and contactless classroom automation. *International Journal of Engineering Research & Technology, 14*(7). https://doi.org/10.5281/zenodo.18104042

Kim, M., Lee, J., & Paek, J. (2018). Neutralizing BLE beacon-based electronic attendance system using signal imitation attack. *IEEE Access, 6*, 77921–77930. https://doi.org/10.1109/ACCESS.2018.2884488

Kişisel Verileri Koruma Kurumu. (2016). *Kişisel Verilerin Korunması Kanunu*. Erişim tarihi: 20 Mayıs 2026, https://www.kvkk.gov.tr/

Madhu, B. G. (2025). Mobile based GPS attendance system. *International Journal for Research in Applied Science and Engineering Technology, 13*(11), 3024–3028. https://doi.org/10.22214/ijraset.2025.75753

Mobile Security Framework. (2026). *YOKSAVAR PRO Android static analysis report: MobSF v4.5.0* [Static analysis report]. https://drive.google.com/file/d/1-G4Gec8vFGuvyyfqsk4YhGYTUJ7MhvNC/view?usp=sharing

Munivrana, L., Pleština, V., & Gotovac, S. (2025). Smarttendance: A BLE-based mobile application for real-time student attendance tracking. In *2025 10th International Conference on Smart and Sustainable Technologies (SpliTech)* (pp. 1–6). IEEE. https://doi.org/10.23919/SpliTech65624.2025.11091720

Nagarajan, G., & Mozhi, V. (2025). Attendance system using Bluetooth Low Energy with smart wearable devices. *AIP Conference Proceedings, 3257*(1), 020156. https://doi.org/10.1063/5.0265094

Napkin AI. (2024). *Napkin AI*. Erişim tarihi: 20 Mayıs 2026, https://www.napkin.ai/

Noguchi, S., Niibori, M., Zhou, E., & Kamada, M. (2015). Student attendance management system with Bluetooth Low Energy beacon and Android devices. In *2015 18th International Conference on Network-Based Information Systems* (pp. 710–713). IEEE. https://doi.org/10.1109/NBiS.2015.109

Özcan, C., Saray, F., & Tari, M. (2018). Mobil cihazlar için RFID & Bluetooth düşük enerji teknolojisi ile öğrenci yoklama sistemi tasarımı. *International Journal of Multidisciplinary Studies and Innovative Technologies, 2*(1), 26–30.

Patel, P. (2026). Revolutionizing academic management: A digital approach to location-based QR attendance system and mobile application integration for lecture and laboratory oversight. In S. Goswami, S. Saha, R. S. Beed, & K. Basu (Eds.), *Data management, analytics and innovation* (Lecture Notes in Networks and Systems, Vol. 1370, pp. 267–284). Springer. https://doi.org/10.1007/978-981-96-6537-2_18

Phan, S., Srun, C., Chhay, P., Pheng, M., Sreng, V., & Thuol, S. (2025). NFC-based on IoT student attendance system: A comparative analysis of artificial neural networks and random forest. In *2025 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA)*. IEEE. https://doi.org/10.1109/ICCIAA65327.2025.11012992

Priem, J., Piwowar, H., & Orr, R. (2022). OpenAlex: A fully-open index of scholarly works, authors, venues, institutions, and concepts. *arXiv*. https://arxiv.org/abs/2205.01833

Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. *Computers & Education, 128*, 13–35. https://doi.org/10.1016/j.compedu.2018.09.009

Sezdi, E., & Tüysüz, B. (2018). Elektronik bilgi sistemleri tabanlı öğrenci yoklama kontrol sistemi. *Bilgi Yönetimi, 1*(1), 23–31. https://doi.org/10.33721/by.398269

Shaikh, S., Gupta, S., Singh, A., Pal, S., & Sheikh, K. (2026). Bluetooth-based smart attendance system using BLE and mobile devices. *International Journal of Engineering Research & Technology, 15*(4). https://doi.org/10.5281/zenodo.19482324

Supabase. (2022, 31 Mart). *Edge Functions are now available in Supabase*. Erişim tarihi: 20 Mayıs 2026, https://supabase.com/blog/supabase-edge-functions

Supabase. (2022, 22 Kasım). *Flutter authorization with RLS*. Erişim tarihi: 20 Mayıs 2026, https://supabase.com/blog/flutter-authorization-with-rls

Surve, P., Patwa, K., & Singh, M. (2025). QR code attendance automation using Flutter. *Journal of Emerging Technologies and Innovative Research, 12*(2). https://www.jetir.org/papers/JETIR2502505.pdf

Szolga, L. A., Arsad, N., & Majumdar, S. (2025). NFC-based smart card systems for educational applications: Design, implementation, and integration. *International Journal of Education and Information Technologies, 19*, 153–159. https://doi.org/10.46300/9109.2025.19.16

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. Erişim tarihi: 20 Mayıs 2026, https://sdgs.un.org/2030agenda

Üçgün, H., İleri, E., Yüzgeç, U., & Yayla, R. (2018). Development of microcontroller based two stage student attendance management system. *Academic Perspective Procedia*, *1*(1), 429-437. https://doi.org/10.33793/acperpro.01.01.86

EXTENDED ABSTRACT

YOKSAVAR PRO: A MULTI-LAYER MOBILE ATTENDANCE SYSTEM BASED ON DEVICE SEALING

This study presents YOKSAVAR PRO, a mobile-based digital attendance system developed to address persistent challenges in higher education attendance processes, including time inefficiency, data unreliability, and proxy attendance. Unlike existing solutions that rely on single-layer verification mechanisms such as QR codes, BLE beacons, or RFID readers alone, YOKSAVAR PRO integrates six distinct security layers within a unified mobile architecture: Bluetooth Low Energy (BLE) proximity verification, Near Field Communication (NFC) card matching, biometric authentication, one-time token verification, device sealing, and real-time push notifications. The system operates entirely on existing mobile devices without requiring additional classroom hardware such as standalone beacon devices, RFID readers, or cameras, thereby offering a cost-effective and scalable solution aligned with Education 4.0 principles and the United Nations Sustainable Development Goals (SDG-4 and SDG-9).

Developed using Flutter for cross-platform compatibility, Supabase PostgreSQL with Row-Level Security for cloud database management, and Firebase Cloud Messaging for notification delivery, YOKSAVAR PRO ensures that students can submit attendance only through their registered device and paired NFC card. The instructor selects a course from the mobile application, starts BLE broadcasting using the flutter_blue_plus library, and generates a unique session ID and session-specific UUID. Students then complete a mandatory four-step verification sequence: biometric authentication via the local_auth library to confirm device ownership, NFC card verification using nfc_manager to match the card's UID against the stored profile, BLE proximity verification to ensure physical presence in the classroom, and one-time token entry to bind the submission to the active session. Only upon successful completion of all four steps does the system record an attendance entry.

A critical security component, device sealing, uses the device_info_plus library to collect hardware fingerprints (ANDROID_ID, model, manufacturer on Android; identifierForVendor on iOS) and associates them with the student's profile along with the NFC card UID. Any subsequent attempt from a different device or card is automatically rejected, effectively preventing cross-device attendance, card sharing, and proxy submissions. Legitimate changes can be reset via an admin web panel built

with Flutter Web and hosted on Firebase Hosting, which also supports course management, CSV-based bulk import/export, exemption status updates, and attendance reporting.

After the instructor closes the session, a Supabase Edge Function triggers automatically, queries the attendance table, and sends personalized push notifications through Firebase Cloud Messaging, delivering confirmations or absence alerts. In experimental tests with 10 different Android devices (9 students and 1 instructor) across 20 sessions, the system achieved a 95% overall success rate, with an average total verification time of 27.63 seconds, BLE detection time of 1.42 seconds, and notification latency of approximately 23 seconds for student devices. The instructor device received notifications within approximately 4–5 seconds, while the higher latency for students is attributed to the Edge Function processing. Device sealing blocked 100% of unauthorized proxy attempts.

A static security analysis of the Android APK using Mobile Security Framework (MobSF v4.5.0) yielded a score of 78/100 (LOW RISK, Grade A), with no high-severity vulnerabilities detected, confirming the application's robust security posture. Compared with existing systems in the literature, none of which simultaneously implement BLE, NFC, biometric, token, device sealing, and notification layers, YOKSAVAR PRO addresses the vulnerability of single-layer BLE systems to signal imitation attacks by making BLE verification necessary but not sufficient for successful attendance submission.

Future work will include offline mode for weak internet connectivity, dynamic short-lived token mechanisms, WiFi based supplementary verification with privacy safeguards, iOS-specific refinements for Core NFC and Face ID, and multitenant support for different institutions. In conclusion, YOKSAVAR PRO offers an integrated, hardware-free, and security-conscious digital attendance solution that aligns with Education 4.0, SDG-4 (Quality Education), and SDG-9 (Innovation and Infrastructure), providing a defensible design against proxy attendance and spoofing attacks while respecting data protection regulations such as Türkiye's KVKK No. 6698.