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.

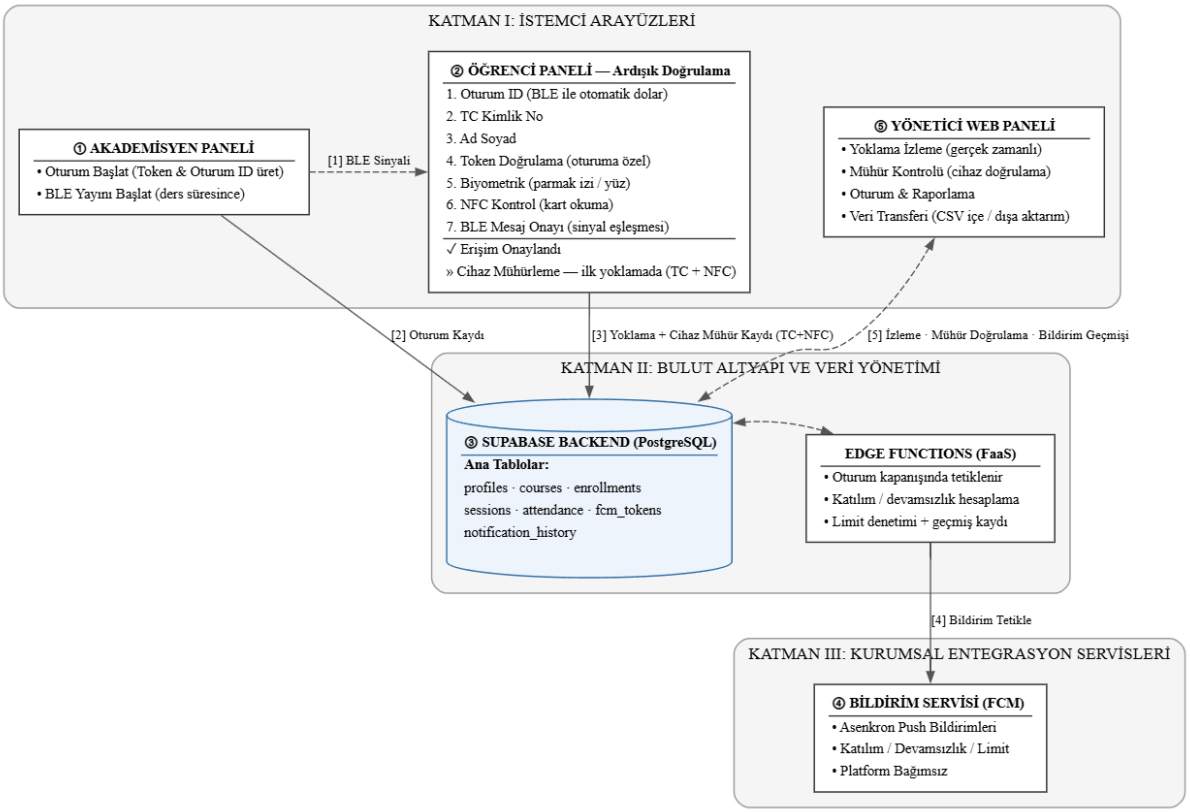
Çalışmanın bir diğer ayırt edici yönü, yoklama oturumu tamamlandıktan sonra öğrencilerin katılım durumlarına ilişkin anlık bildirim alabilmesidir. Literatürde yer alan çalışmaların önemli bir bölümü yalnızca yoklama kaydının alınmasına odaklanırken, YOKSAVAR PRO yoklama sonrasındaki bilgilendirme sürecini 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

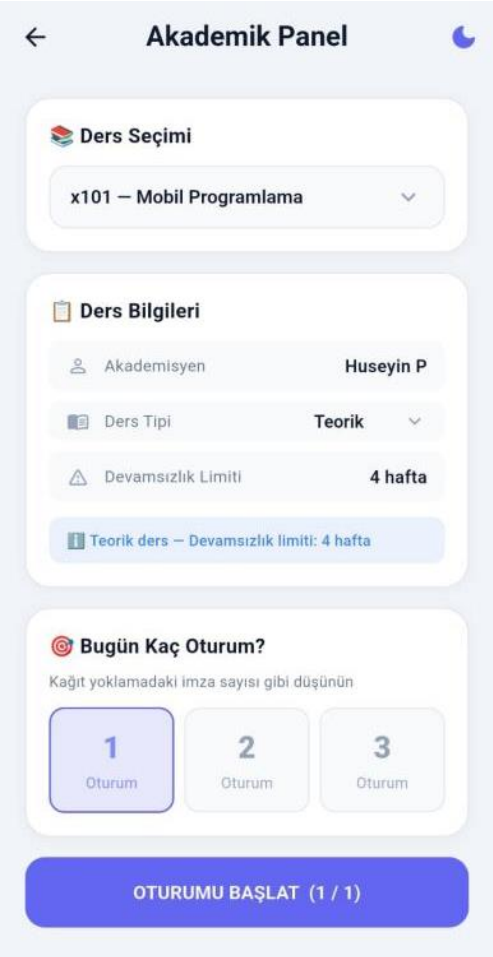
cihaz yelpazesinde sorunsuz çalışabilme açısından önemli bir avantaj sağlamaktadır. BLE iletişimi için flutter_blue_plus, NFC işlemleri için nfc_manager, biyometrik doğrulama için local_auth ve cihaz mühürlemede kullanılan donanım kimlik bilgileri için device_info_plus kütüphaneleri kullanılmıştır. device_info_plus 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.



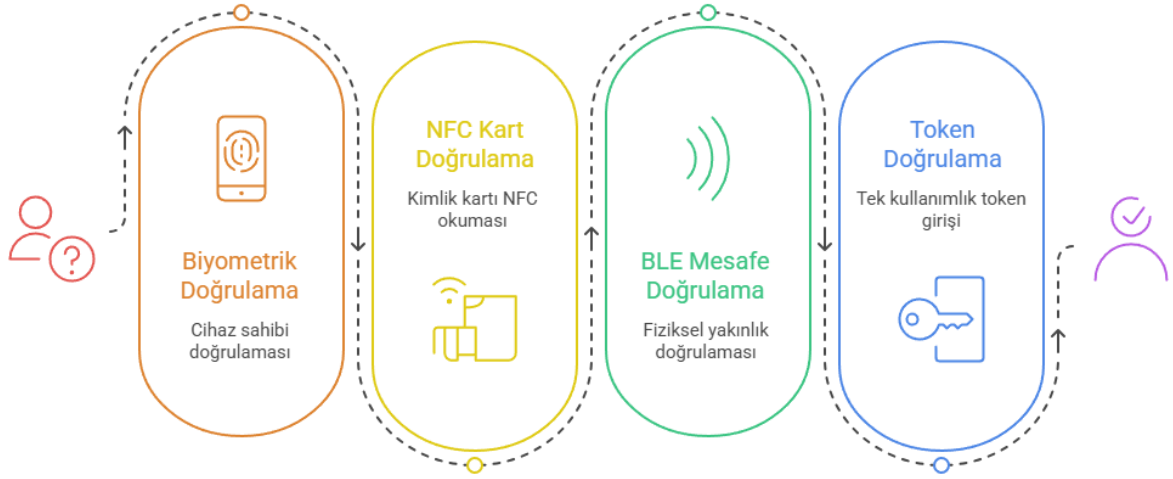
Şekil 2. Akademisyen Paneli: Ders Seçimi ve Canlı Oturum Görünümü

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.

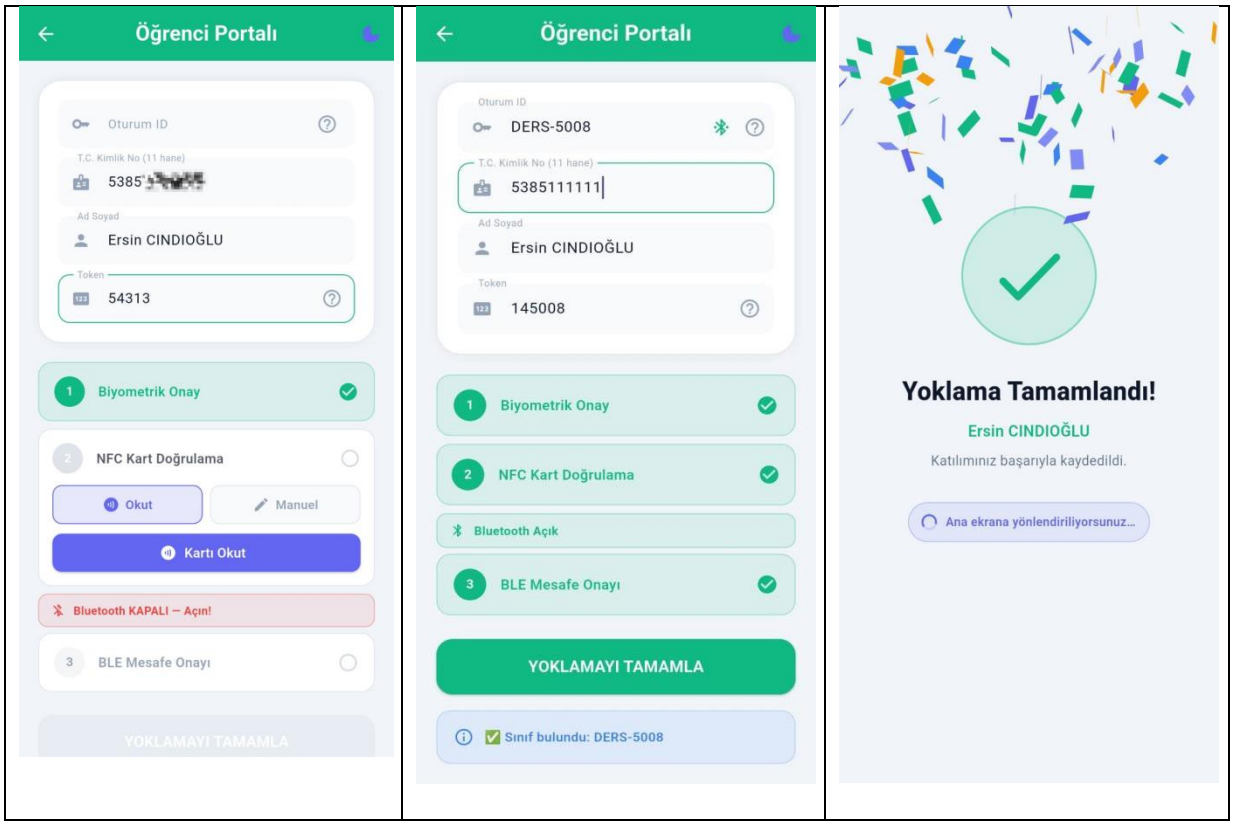
İkinci aşama olan NFC kart doğrulama adımında, öğrencinin kimlik kartının veya kendisine tanımlanmış NFC etiketinin mobil cihaz aracılığıyla okutulması sağlanmaktadır. Sistem, karttan elde edilen Unique Identifier (UID) değerini, veritabanında öğrenci profiliyle ilişkilendirilmiş kayıtlı NFC UID bilgisiyle 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,

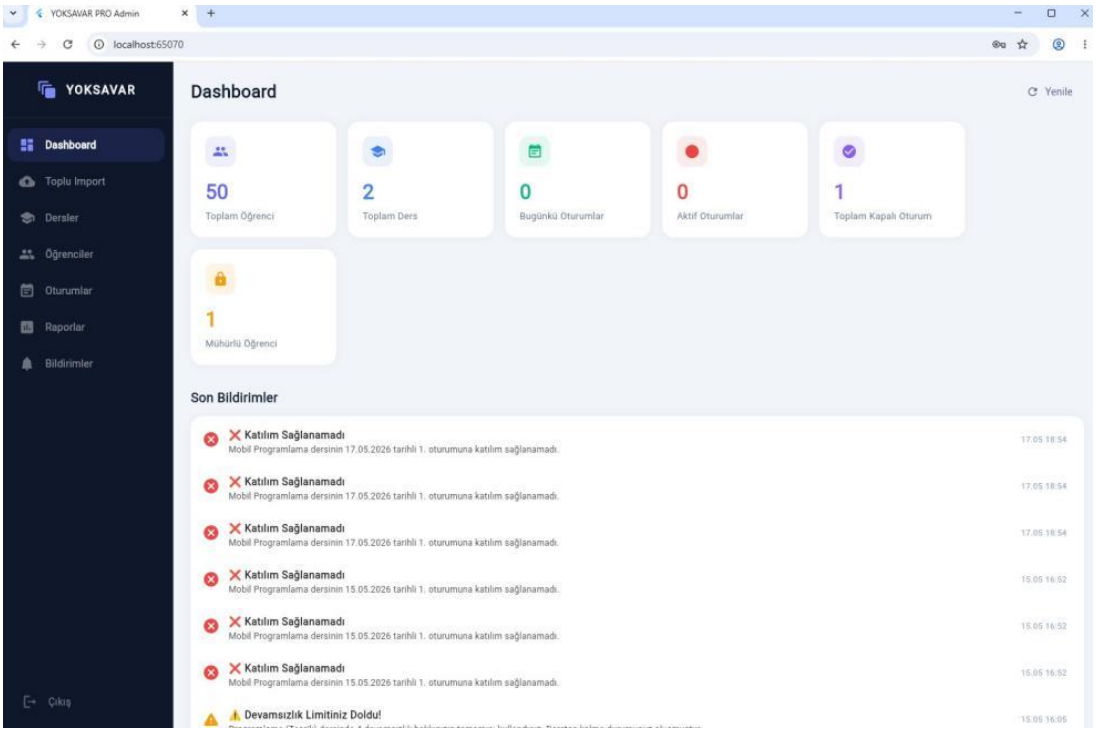
"Ahmet Y******"); raporlama amacıyla gerçekleştirilen dışa aktarma işlemlerinde ise alan bazlı erişim yetkilendirmesi uygulanmaktadır. Bu yaklaşım, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun veri minimizasyonu ilkesiyle uyumludur. Öğrencilere ait cihaz mühürleme bilgileri ve NFC kart UID kayıtları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

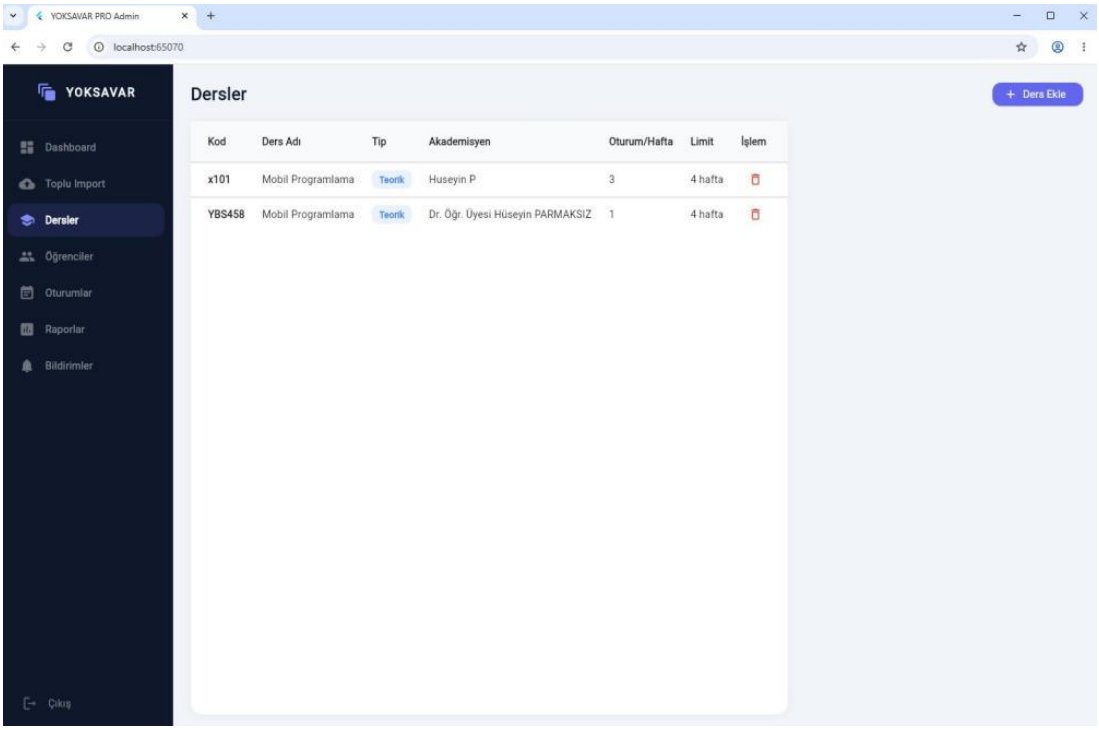
Kurumsal kart altyapısının yeterli olmadığı veya test ortamlarında harici kart okuma ve yazma gereksiniminin ortaya çıktığı durumlarda Arduino uyumlu NFC/RFID okuyucu modülleri alternatif çözüm olarak değerlendirilebilmektedir. Arduino Store'da yer alan NFC/RFID Reader with Two Transponders ürünü bu 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.

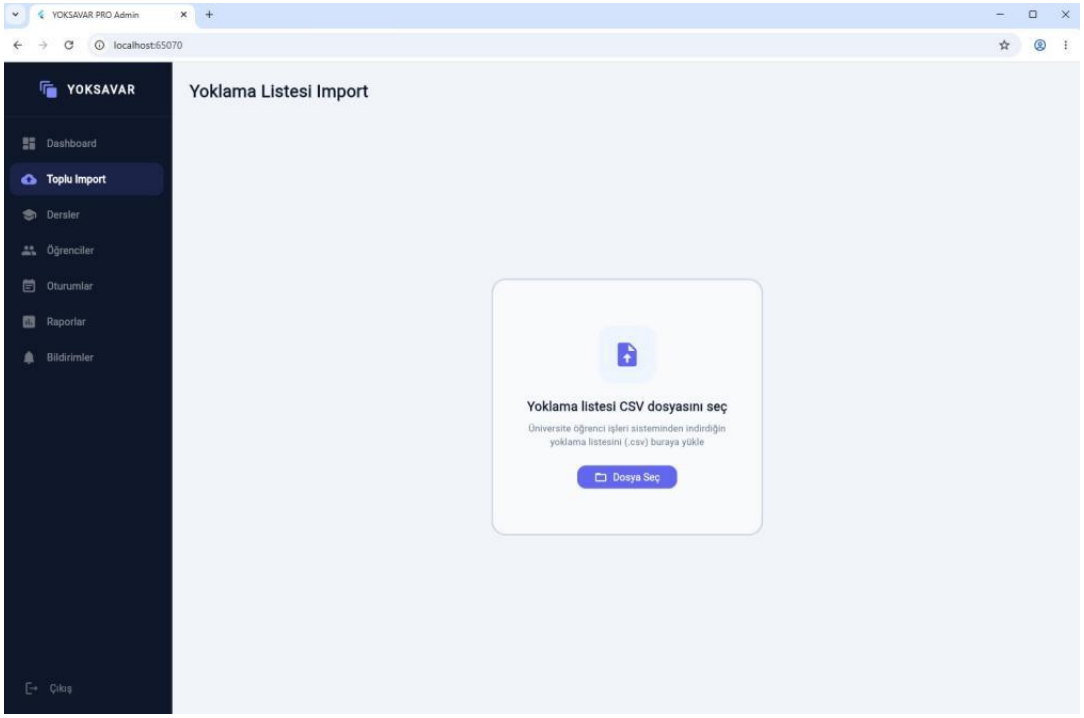
Muafiyet durumu güncelleme özelliği sayesinde belirli öğrenciler devamsızlık hesaplamalarından muaf tutulabilmektedir. Bu özellik, sağlık raporu veya geçerli mazeret gibi durumların sistem üzerinden etkin biçimde yönetilebilmesine olanak sağlamaktadır.



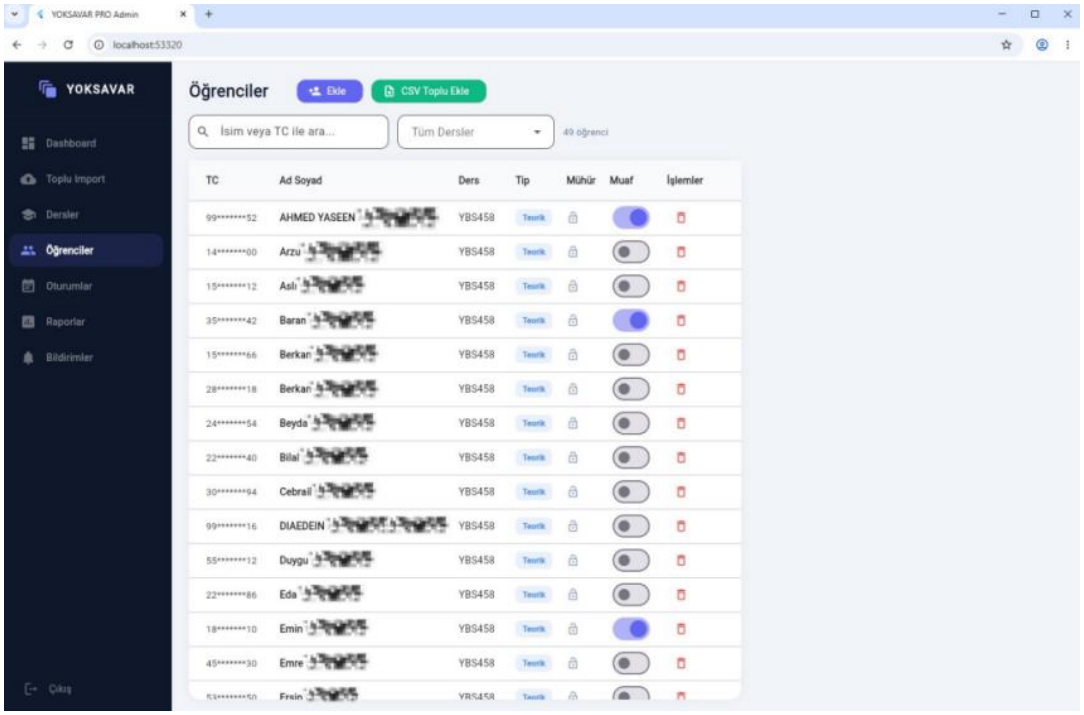
Şekil 5. Admin Web Paneli



Şekil 6. Admin Web Paneli: Ders Yönetimi



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



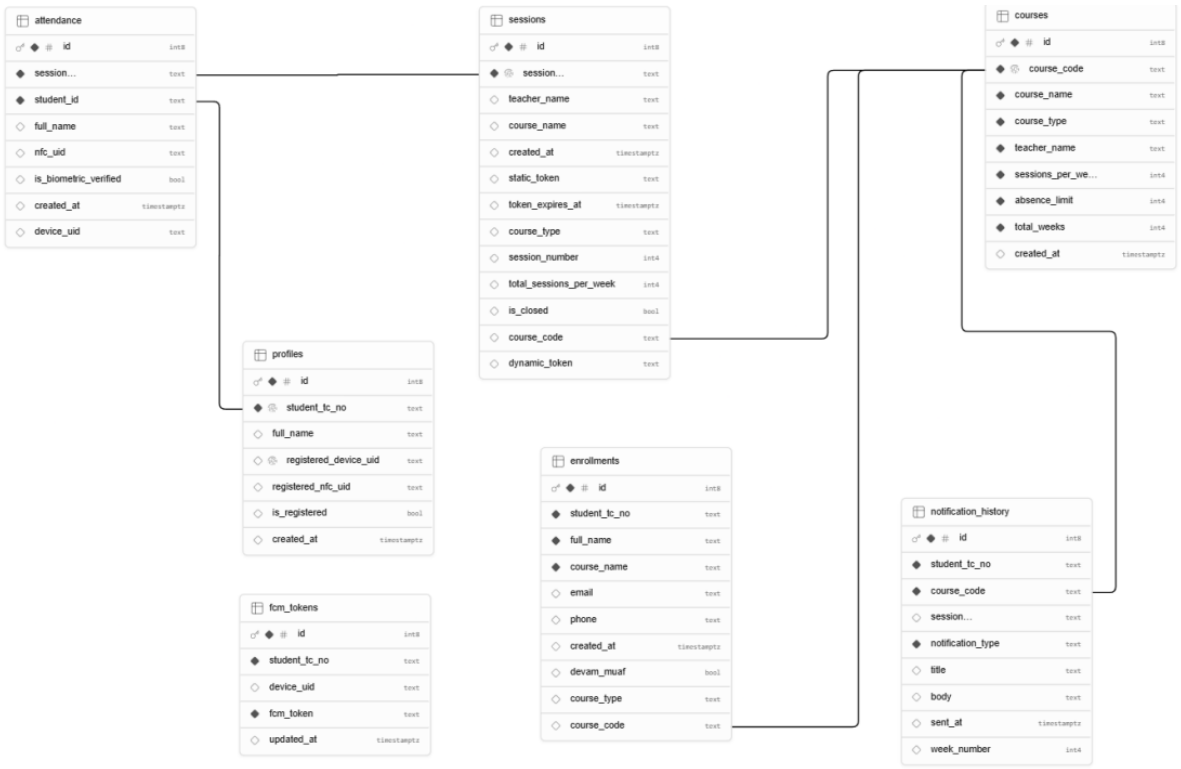
Şekil 8. Admin Web Paneli: Muafiyet Durumu Güncelleme ve Devamsızlık Raporları Ekranı

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.

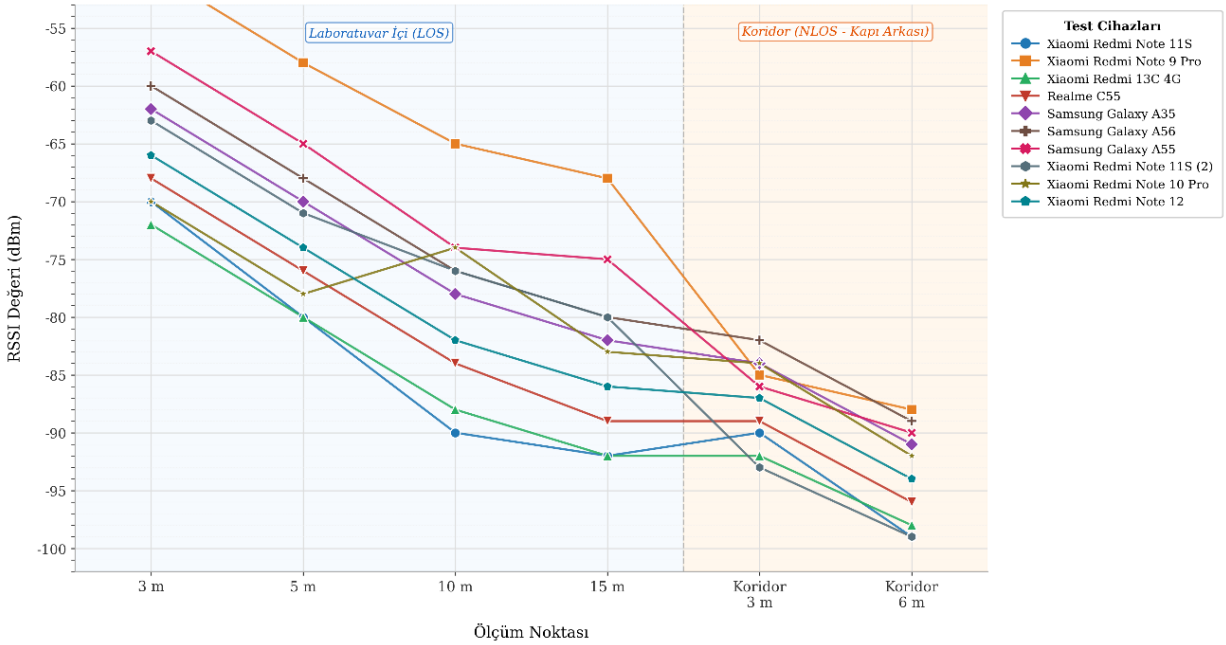
4.3. Cihaz Mühürleme Performansı

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.