MAKÜ|MMF
MÜHENDİSLİK-MİMARLIK FAKÜLTESİ

Uluslararası Mühendislik, Tasarım ve Teknoloji Dergisi, 2024, 6(1), Sayfa: 22-30
International Journal of Engineering, Design and Technology, 2024, 6(1), Page: 22-30

Araştırma Makalesi
Research Article

Uygulama, altyapı ve ağ gözlenebilirlik platformunun geliştirilmesi

Development of an application, infrastructure, and network observability platform

Oğuzhan Demir[1], Ahmet Can Uğur[1], Mehmet Burak Deveci[1], Mehmet Fatih Akay[2], Ceren Ulus[2*]

[1]Trendyol, Teknoloji Departmanı, İstanbul, Türkiye
[2]Çukurova Üniversitesi, Bilgisayar Mühendisliği Departmanı, Adana, Türkiye

Özet: Gözlenebilirlik, bir sistemin iç durumlarının, çıktılarına bakılarak tahmin edilme derecesini ifade eder. Bir sistemin gözlenebilir olması, o sistemin tüm iç durumlarının dışarıdan alınan ölçümlerle tam olarak belirlenebilmesini sağlar. Uygulama, altyapı ve ağ gözlenebilirliği, kontrol teorisi ve otomatik kontrol sistemleri tasarımında kritik bir rol oynar. Bu özellik, sistemin kontrol edilip edilemeyeceğini belirler. Bu çalışmada, tüm teknoloji katmanlarının performansını olumsuz etkileyen olayları ve standart dışı durumları anlamak ve eyleme dönüştürülebilir akıllı bildiriler sağlamak için uygulama, altyapı ve ağ gibi sistemlerin gözlenebilirlik verilerini tek bir platform aracılığıyla toplayan, anlık gözlenmesini, ilişkilendirilmesini, standartlaştırılmasını ve analiz edilmesini sağlayan bir platform geliştirilmiştir. Bu sayede, kullanılan birden fazla alternatif ve sadece kısmi işlev gören platformlar yerine, tek bir platform ile tüm gözlenebilirlik ihtiyaçları karşılanmış ve bütünleşik bir gözlenebilirlik deneyimi sunulmuştur. Platform kapsamında, çeşitli sistemlerden ilgili telemetri (log, metrik, iz, olay) verilerini alan, kaydedip saklayan, görselleştirip raporlanmasını sağlayan, belli durumlarda alarm üreten, akıllı alarm yöntemleri ile destekleyen, bir sorunun temel nedenini belirlemek ve çözmek amacıyla kullanılan bir yaklaşım olan kök neden analizi ile sorunların kök nedenlerini kolayca bulmayı sağlayan araçlar, web servisleri, kullanıcı arayüzleri ve makine öğrenme modelleri geliştirilmiştir. Bu platform, kullanıcılarına bütünleşik bir gözlenebilirlik çözümü sunmaktadır. Ayrıca, geliştirilen platform ile gözlenebilirlik platformu kullanıcı sayısının %30 arttığı gözlenmiştir.

Anahtar Kelimeler: Gözlenebilirlik, Entegre Platform, Açık Kaynak Teknolojileri, Kök Neden Analizi

Abstract: Observability refers to the degree to which the internal states of a system can be predicted by looking at its outputs. The observability of a system ensures that all internal states of that system can be precisely determined by external measurements. Application, infrastructure and network observability plays a critical role in control theory and automatic control systems design. This feature determines whether the system can be controlled or not. In this study, a platform has been developed that collects observability data of systems such as applications, infrastructure and networks through a single platform and enables instant observation, association, standardization and analysis in order to understand events and non-standard situations that negatively affect the performance of all technology layers and to provide actionable smart notifications. In this way, instead of using multiple alternatives and only partially functional platforms, all observability needs are met with a single platform and an integrated observability experience is offered. Within the scope of the platform, it is an approach that receives relevant telemetry (log, metric, trace, event) data from various systems, records and stores it, visualizes and reports it, generates alarms in certain situations, supports it with smart alarm methods, and is used to determine and solve the root cause of a problem. Tools, web services, user interfaces and machine learning models have been developed to easily find the root causes of problems through cause analysis. This platform offers its users an integrated observability solution. Additionally, it has been observed that the number of observability platform users increased by 30% with the developed platform.

Keywords: Observability, Integrated Platform, Open Source Technologies, Root Cause Analysis

1. Giriş

Gözlenebilirlik, karmaşık sistemlerin iç durumlarını dış gözlemler yoluyla anlama yeteneğidir. Bu kavram, sistemlerin performansını izlemek, sorunları tespit etmek ve çözmek için hayati öneme sahiptir. Uygulama gözlenebilirliği, yazılım uygulamalarının performansını ve davranışını izlemeyi kapsamaktadır. Bu süreç, uygulamanın performansını, hata oranlarını, kullanıcı davranış-

* İletişim Yazarı / *Corresponding author*. Eposta/*Email* : f.cerenulus@gmail.com
Geliş / *Received*: 12.07.2024, Revizyon / *Revised*: 14.07.2024
Kabul / *Accepted*: 19.07.2024

Burdur Mehmet Akif Ersoy University Press

larını ve diğer önemli metrikleri izlemeyi içermektedir. Uygulama içinde gerçekleşen işlemleri ve etkileşimleri anlamak için çeşitli metriklerin, logların ve izlerin toplanmasını ve analiz edilmesini sağlamaktadır. Bu sayede, kullanıcı deneyimi iyileştirilmekte ve uygulama kesinti süreleri azaltılmaktadır. Altyapı gözlenebilirliği, uygulamaların çalıştığı fiziksel ve sanal kaynakların performansını ve durumunu izlemeyi kapsamaktadır. Bu özellik, sunucular, veritabanları, konteynerler, sanal makineler ve bulut hizmetleri gibi bileşenleri içermektedir. Sunucuların çalışma verimliliğini ve performans sorunlarını tespit etmek için Merkezi İşlem Birimi (MİB) kullanımı, bellek kullanımı, disk Giriş/Çıkış (G/Ç) ve ağ trafiği gibi metrikler izlenmektedir. Ağ gözlenebilirliği, ağ trafiğini ve ağ bileşenlerinin performansını izlemeyi kapsamaktadır. Bu kavram, ağ geçitleri, yönlendiriciler, anahtarlar, güvenlik duvarları ve yük dengeleyiciler gibi ağ cihazlarının izlenmesini içermektedir.

Altyapıların yönetimi ve performansının sağlanması, operasyonel verimlilik ve müşteri memnuniyeti açısından kritik bir öneme sahiptir. Gözlenebilirlik amacıyla kullanılan çeşitli lisanslı ve açık kaynak ürünler ile çözümler, birbirinden bağımsız ve dağınık bir yapıda bulunmaktadır ve yüksek lisans maliyetleri ve uygulama işgücü gerektirmektedir. Bu yapı, uçtan uca bütünsel bir gözlenebilirlik sağlamaktan uzak olup, sorunların kök nedenlerine inmek ve hızlı aksiyon almak konusunda önemli zorluklara sebep olmaktadır. Olası bir sorun meydana geldiğinde, birden fazla sisteme giriş yapmak ve her bir sistemdeki verileri analiz etmek gerekmektedir. Bazı durumlarda, bütünsellik ve ilişkilendirme eksikliği nedeniyle sorunları tespit etmek ve çözüm üretmek neredeyse imkansız hale gelmektedir. Bu durum, hem zaman kaybına hem de yüksek maliyetlere yol açarak operasyonel verimliliği düşürmekte, müşteri deneyimi üzerinde olumsuz etkiler yaratmakta ve rekabet gücünü zayıflatmaktadır.

Bu çalışmada, uçtan uca uygulama seviyesinden fiziksel donanım seviyesine kadar olan süreçler bütünleşik bir şekilde yönetilebilen ve ilgili kullanıcılar tarafından özelleştirilmiş panellerle izlenebilen ve yapay zeka destekli akıllı mekanizmalar içeren, problemler için uyarı sistemleri oluşturabilen ve problemlerin kök ve etki analizini yapabilen bir uygulama, altyapı ve ağ gözlenebilirlik platformu geliştirilmesi amaçlanmıştır.

Çalışma ilgili literatür, platformun detayları, çalışmanın sonuçları ve sonuç bölümü olarak organize edilmiştir.

2. Literatür İncelemesi

Princz ve ark. (2024), çeşitli makine öğrenimi modellerini kullanarak ikili zaman serisi verilerinde anomali tespiti için bir analiz sunmuştur. Çalışma kapsamında veri setinin ön işlenmesi, verilerin normalleştirilmesi ve farklı modellerin anomali tespit performansının değerlendirilmesi yapılmıştır. Değerlendirme ölçütleri olarak doğruluk, tespit oranı ve F1 puanı kullanılmıştır. Sonuçlar ele alındığında, performans ve hesaplama verimliliği arasındaki takaslar vurgulanmış ve gerçek zamanlı uygulamalarda daha fazla araştırma potansiyeline değinilmiştir.

O'Leary (2023), zaman serisi verileri için özellikle tahmin ve anomali tespiti alanlarında otomatik makine öğrenimi yazılımlarına genel bir bakış sunmuştur. 28 farklı ölçüt ele alınarak işlevsellik, kod olgunluğu ve topluluk desteği değerlendirilmiştir. Zaman serisi verilerinin analizi, tahminlerin yapılması, anomali tespiti ve veri keşfi alanlarında birçok araştırma ve uygulama imkanı sunduğu belirtilmiştir.

Blanco (2023), modern dağıtılmış sistemlerde gözlenebilirliğin önemi ve OpenTelemetry standartlarının telemetriyi sinyaller ve hizmetler arasında ilişkilendirerek dağıtılmış sistemleri anlamak için bütünsel bir yaklaşım sağladığını vurgulayan bir çalışma yapmıştır. Bireysel sinyallerin (izler, sinyaller ve günlükler) belirli kullanım durumları için sahip oldukları özellikler açıklanmış ve bu sinyallerin bağlam olmadan izole bir şekilde kullanıldığında yararlılıklarının azaldığı belirtilmiştir. Gözlenebilirliğin gerçek değerinin, mühendislik ekiplerinin tüm sinyallerden yararlanarak hizmetlerini buna göre enstrümanlaştırmaları ve hata ayıklama iş akışlarında telemetri bağlamını kullanmaları durumunda ortaya çıkacağı ifade edilmiştir.

Pintilie ve ark. (2022), çok değişkenli zaman serilerinde (MTS) anormallik tespiti (AD) için difüzyon modellerinden yararlanma üzerine çalışmalar yürütmüştür. Bu çalışmalarda iki difüzyon tabanlı model test edilmiş ve birkaç sinirsel temel çizgiyle karşılaştırılmıştır. Test edilen difüzyon tabanlı modellerin, sentetik veri kümelerinde temel çizgilere kıyasla daha üstün bir performans sergilediği gözlenmiştir. Bu sonuçlar, difüzyon tabanlı yöntemlerin çok değişkenli zaman serilerinde anormallik tespiti için potansiyelini ortaya koymuştur.

Dilib Kumar Sharma ve ark. (2022), mevcut akıllı otomasyona ilişkin bilimsel girdilerin sistematize edilmesi ve bunların performans yönetimi zorluklarına temel katkılarının aydınlatılması amacıyla bir çalışma yapmıştır. Uluslararası işletme (International Business - IB), genel yönetim (General Management - GM), bilgi yönetimi (Information Management - IM) dergilerinde ve performans yönetimi (Performance Management - PM) ortamlarında yapay zeka, robotik ve diğer teknolojik konularda araştırmalar yapılarak 45 yayın incelenmiştir. Sonuçlar, akıllı otomasyon teknolojilerinin personel yönetimi ve şirket performansının iyileştirilmesi için yeni bir strateji ve çeşitli performans yönetimi fırsatları sağladığını, ayrıca teknolojik ve etik sorunların ortaya çıkarıldığını göstermektedir.

Alimohammadi ve Nancy Chen (2022), zaman serisi verilerinin borsa, teşhis, meteoroloji, petrol ve gaz endüstrisi gibi birçok disiplinde toplanıp analiz edildiğini belirtmiştir. Zaman serilerinde aykırı değer tespiti için istatistiksel, regresyon tabanlı ve makine öğrenimi tabanlı kategorilere ait toplam 17 teknik, petrol ve gaz üretimi veri analizine uygulanmıştır. Bu yöntemlerden

15'inin üretim verisi analizinde ilk kez kullanıldığı belirtilmiştir. Tekniklerin performanslarının belirlenebilmesi için Doğruluk, Kesinlik, Geri Çağırma ve F1 Puanı gibi ölçütler kullanılmıştır.

Bahri ve ark. (2022), denetimsiz anormallik tespiti için önerilen otomatik yöntemler ve stratejiler vurgulanarak Otomatik Makine Öğrenimi (OML) alanında araştırmalar yapmıştır. Çalışmada, makine öğrenimi algoritmalarının kullanımının daha erişilebilir hale getirilmesi amacıyla OML'nin kullanılması önerilmiştir.

Manchanda (2021), kurumsal bilgi sistemlerindeki performans sorunlarının, eğilimlerinin ve sistem arızalarının izlenmesi, tahmin edilmesi ve önerilmesi için makine öğrenimi algoritmalarını kullanan bir sistem sunmuştur. Bu sistemde, uygulamaların dağıtılmış erişimi ve kontrolü ile kuruluşların farklı uygulamaların genel durumunu korumalarına yardımcı olunmuştur.

Hashemnia ve ark. (2021), yenilenebilir enerji sektöründe, tek bir bileşen arızasının tüm ağın performansını etkileyebilmesi nedeniyle, arızaların tahmin edilmesi ve veri ile zamana dayalı bakımdan daha fazla koşula geçişi kolaylaştırmak amacıyla yapay zeka tabanlı makine öğrenimi tekniklerinin kullanılmasını önermiştir. Makine öğreniminin sektör uzmanlığıyla birlikte belirli arıza modları ve bileşenler için arıza olasılığını nasıl tahmin edebileceği açıklanmıştır. Bileşen arızasının meydana geldiği bir vaka çalışması ele alınarak belirli bir arıza modu gösterilmeye çalışılmıştır. Sorunun iki aşamalı bir teknik kullanılarak çözüleceği açıklanmıştır. İlk olarak, mevcut değeri verilerek parametrenin gelecekteki olasılık dağılımı tahmin edilmiş, ikinci olarak ise tahmin edilen parametre değeri verilerek arıza olasılığı belirlenmiştir. Bu sayede teknik bileşenlerin arızalarının önceden tahmin edilmesi ve Kalan Kullanım Ömrü'nün (KKÖ) belirlenmesi için standartlaştırılmış bir yaklaşıma olanak sağlanmıştır.

Tang ve ark. (2021), uygulamaların darboğazlarını tespit etmek, çalışma zamanındaki davranışlarını izlemek ve olası güvenlik risklerini belirlemek amacıyla kullanılan Uygulama Performans Yönetimi (UPY) kitaplıklarını incelemiştir. Android uygulamaları için UPY'ler üzerine ilk sistematik çalışma yürütülmüş ve Android uygulamalarında UPY'lerin kullanımını keşfetmek amacıyla APMHunter adında bir çerçeve geliştirilmiştir. APMHunter kullanılarak, UPY'lerin kullanım kalıpları araştırılmış ve olası kötüye kullanımların keşfedilmesi için 500.000 Android uygulaması üzerinde geniş ölçekli deneysel bir çalışma gerçekleştirilmiştir. Bu deneysel çalışmalar sonucunda iki bulgu elde edilmiştir. İlk bulgu, bazı UPY'lerin hala kullanımdan kaldırılmış izinler ve yaklaşımlar kullanıyor olması ve bunun da UPY'lerin beklendiği gibi performans göstermemesine sebep olmasıdır. İkinci bulgu ise, UPY'lerin uygunsuz kullanımının gizlilik sızıntılarına sebep olabileceği yönündedir. Bu bulgular göz önünde bulundurularak, çalışmalarında hem UPY satıcılarının hem de geliştiricilerin UPY'leri titizlikle tasarlamaları ve kullanmaları önerilmiştir.

Onodueze ve Josyula (2021), MIL-STD-1553 iletişim trafiğindeki normal, periyodik olmayan mesajları taklit eden saldırıların tespiti için kullanılan çeşitli makine öğrenimi algoritmalarının yeteneklerini değerlendirmiştir. Veri kümesinde bulunan dengesizlikten dolayı veri kümesinin doğru şekilde sınıflandırılabilmesi amacıyla, veri kümesine uygulanan modellerin performansını değerlendirmek için uygun metrikler belirlenmiştir. Belirlenen metrikler kullanılarak, üretilen farklı makine öğrenimi modellerinin performansları karşılaştırılmıştır.

Schulz ve ark. (2020), Yüksek Performanslı Bilgi İşlem (YPBİ) sisteminin bileşenlerinin performansını karakterize etmek ve sensör verilerine dayanarak anormallikleri tanımlamak amacıyla denetimsiz bir makine öğrenme tekniği olan Bayesian Gaussian karışım modelleri üzerine çalışmalar yürütmüştür. Bu amaç doğrultusunda algoritmik bir çerçeve önerilmiştir. Çerçeve, Sayısal Kadastro Veri Tabanı izleme ve operasyonel veri analitiği sistemi içinde uygulanmış ve bir üretim YPBİ sisteminden gelen veriler kullanılarak gerçekleştirilen örnek incelemeler sunulmuştur.

Hagemann ve Katsarou (2020), bulut ölçümlerindeki anormalliklerin tespiti, donanım arızaları, performans darboğazları veya izinsiz girişler gibi sistem sorunlarının kısmen otomatik bir şekilde tespit edilmesi için makine öğreniminin kullanılmasını önermiştir. Anormallik tespitleri iki alanda değerlendirilmiştir. İlk olarak, Yahoo! üzerinde anormallik tespiti için denetimsiz, yeniden yapılandırmaya dayalı Temel Bileşen Analizi, Otomatik Kodlayıcı ve Uzun Kısa Vadeli Bellek (UKVB) – Otomatik Kodlayıcı olmak üzere üç farklı yöntem değerlendirilmiştir. Daha sonra, seçilen modeller yoğunluk temelli yaklaşımla karşılaştırılmış ve yeniden yapılandırma temelli yaklaşımların daha iyi performans gösterdiği açıklanmıştır.

Emamjome ve ark. (2020), veri ön işlemesi için süreç madenciliği metodolojisinin geliştirilmesi ve veri analitiği alanında bilgi sistemleri teorisinin geliştirilmesi için temel oluşturmuştur. Olay günlüğü veri kalitesi sorunlarının temel nedenlerinin ortaya çıkarılması ve belirtilerinin düzeltilmesi amaçlanmıştır.

Qiu ve ark. (2019), zaman serisi temel performans göstergeleri için konvülasyon ve UKVB sinir ağları ile değişken bir otomatik kodlayıcıya dayanan denetimli derin öğrenme modellerine dayalı yeni bir anormallik dedektörü önermişlerdir. Önerilen dedektörün performansı, Yahoo'nun anormallik tespiti için diğer çalışmalarla karşılaştırıldığında A1benchmark ve A2benchmark veri kümelerinde doğruluğunun ve 0.90'ı aşan F1 puanının başarılı bir şekilde sergilendiği belirtilmiştir.

Elsner ve ark. (2019), birden fazla APM sisteminden gelen verilere dayanarak, kurumsal bir uygulamadaki anormallikleri tespit etmek için yoğunluk tabanlı denetimsiz

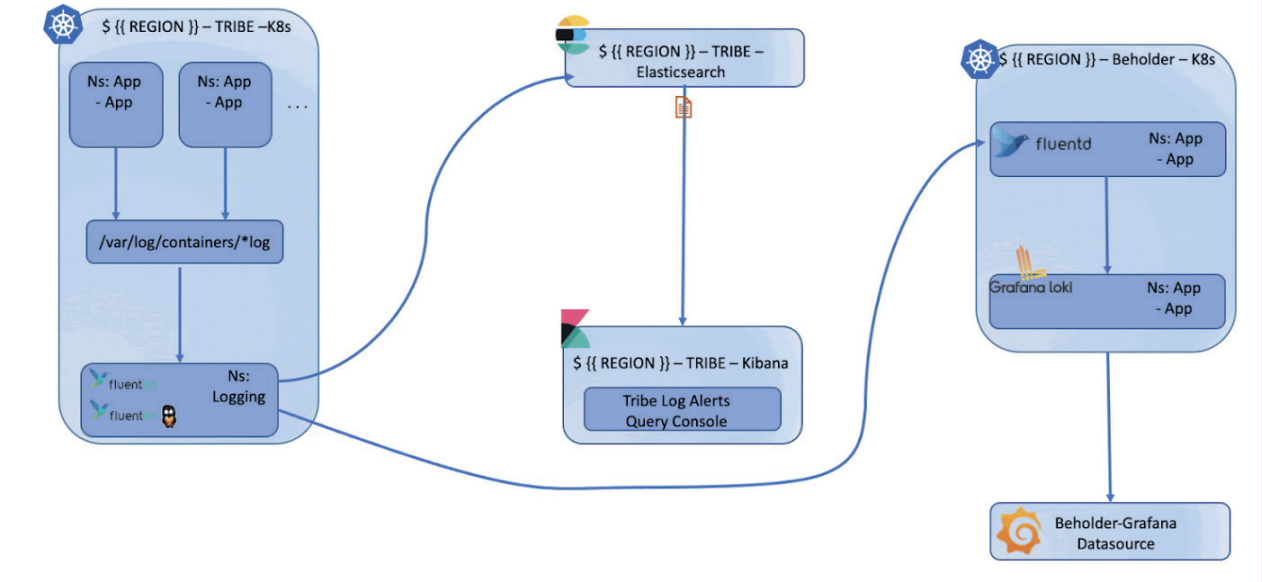
bir makine öğrenimi modeli geliştirmişlerdir. Avrupalı bir otomotiv şirketiyle işbirliği içinde yapılan çalışmada, iki aylık canlı uygulama verileri kullanılarak modelin anormal sistem davranışını başarılı bir şekilde tespit ettiği ve bu tespitin, aykırı değer tespit tekniğinden daha başarılı olduğu ve temel nedenleri belirlemek için bilgi sağladığı gösterilmiştir.

Zhou ve ark. (2019), çevresel yapılandırmalar ve mikroservislerin eş zamanlı etkileşimleri ile ilgili mikroservis arızalarından kaynaklanan zorlukların üstesinden gelmek için sistem izleme günlüklerinin analizine dayalı olarak mikroservis uygulamaları için gizli hata tahmini ve hata yerelleştirme yaklaşımı önermişlerdir. Yürütülen deneysel çalışmalar sonucunda, önerilen yaklaşımın gizli hataları, hatalı mikroservisleri ve hata türlerini uygulama içinde yüksek doğrulukla tahmin edebildiği ve dağıtılmış sistemler için hata teşhisi yaklaşımından daha başarılı performans gösterdiği açıklanmıştır.

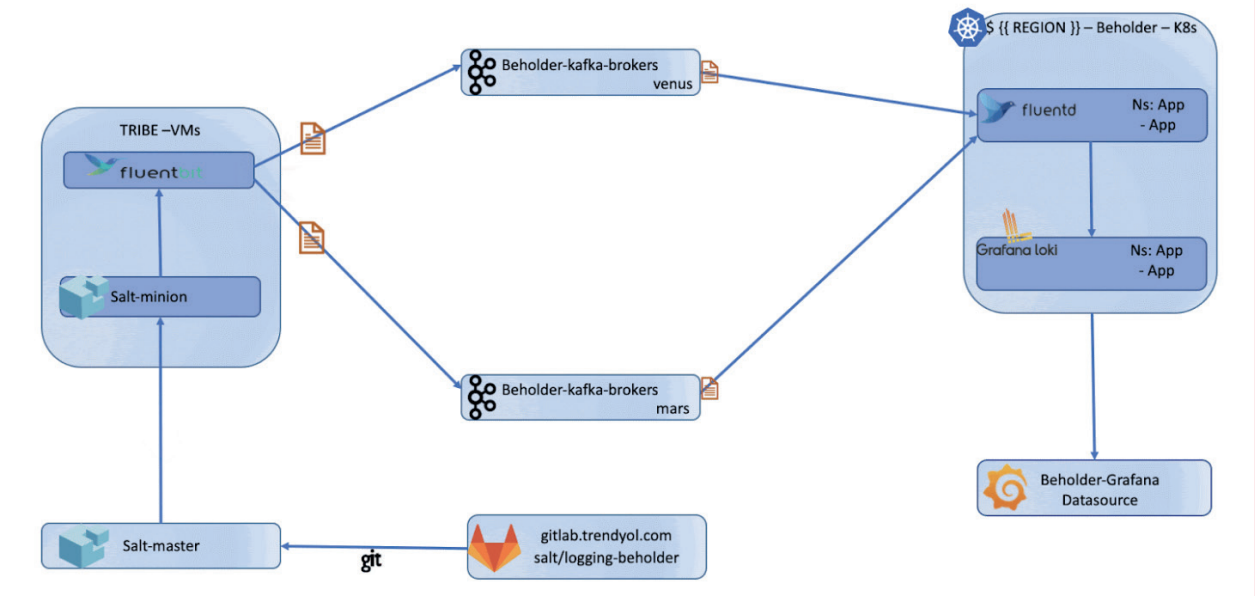
3. Platformun Detayları

Sistem mimarisi ve geliştirmeleri, Trendyol'un hizmetlerini desteklemek ve bu hizmetlerin her katmandaki entegrasyonunu sağlamak için büyük veri toplama sistemini oluşturmuştur. Bu sistem, fiziksel cihaz katmanından başlayarak ağ, sistem altyapısı, platform servisleri ve en uçta bulunan Uygulama Programlama Arabirimi (UPA) servislerine kadar olan ilişkileri sağlamak amacıyla verilerin entegrasyonunu gerçekleştirmektedir.

İlk olarak, tüm telemetri verilerinin (metrikler, log



Şekil 1. Logların alınması ve saklanması için kullanılan mimari.



Şekil 2. Logların alınması ve saklanması için kullanılan mimari.

kayıtları, izlenebilirlik, olaylar) çoklu ortamda toplanıp depolanması amacıyla veri kaynakları servisleri oluşturulmuştur. Logların alınması ve saklanması için kullanılan mimari, Şekil 1 ve Şekil 2'de gösterilmektedir.

Uygulama izlerinin alınması, saklanması ve okunması için kullanılan mimari Şekil 3 ve Şekil 4'te gösterilmektedir.

Uygulama, altyapı ve ağ geliştirme platformu, çeşitli bileşenlerden oluşmaktadır. Bu bileşenler arasında Uygulama Performans İzleme, Altyapı İzleme, Ağ Sistemleri İzleme, Bulut Ortamı ve Performans İzleme, Platform Servis İzleme, Sürekli Profilleme, Görselleştirme ve Raporlama Kullanıcı Arayüzü, Alarm Oluşturma ve Raporlama, Akıllı Anomali Tespiti, Kök ve Etki Analizi, Kullanıcı İzleme, Yapay Zeka İzleme ile yazılım geliştirme kitleri ve kütüphaneler bulunmaktadır. Modüllerin geliştirilmesi ve gözlenebilirlik platformuna entegre edilmesi için Java, Go, .NET ve Node.js kullanılmıştır. Ayrıca, gözlenebilirlik platformunun geliştirilmesi için tüm telemetri verilerinin toplanabileceği açık kaynaklı veri tabanı servisleri, görselleştirme servisleri ve sistemlerin altyapıda birbirleriyle entegrasyonunu sağlayacak yapılar kurulmuştur.

3.1. Uygulama Performans İzleme

Uygulama performans izleme ekranında telemetri verileri (metrikler, loglar ve izler) toplanmakta, analiz edilmekte ve gösterilmektedir.

3.2. Altyapı İzleme

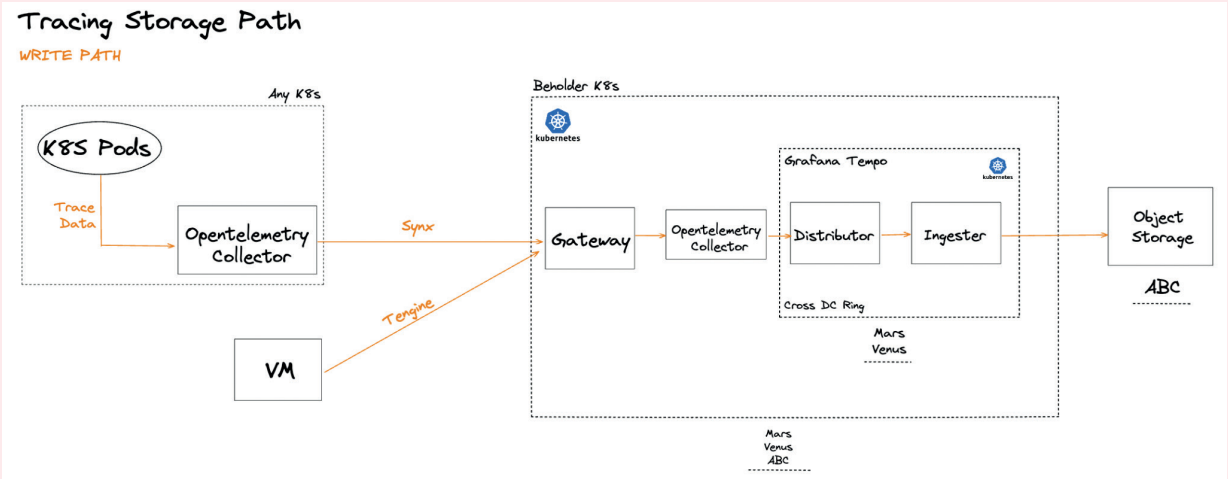
Altyapı izleme ekranında fiziksel cihazlardan başlayarak telemetri verileri (metrikler ve loglar gibi) toplanmakta, bu verilerin entegrasyonu sağlanmakta, analizleri yapılmakta ve ilgili ekranlarda gösterilmektedir. Altyapı İzleme Panosu Şekil 5'te gösterilmektedir.

3.3. Ağ Sistemleri İzleme

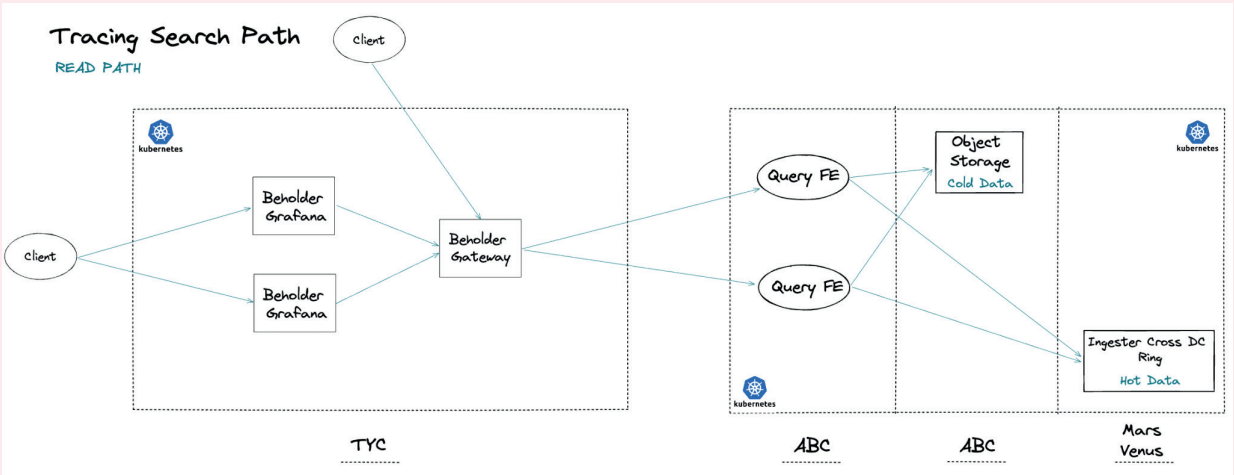
Ağ sistemleri izleme ekranlarının oluşturulabilmesi için fiziksel cihazlardan başlayarak metrik ve log gibi telemetri verileri toplanmakta, bu verilerin entegrasyonu sağlanmakta, analizleri yapılmakta ve ilgili ekranlarda gösterilmektedir.

3.4. Bulut Ortamı ve Performans İzleme

Bulut ortamı ve performans izleme ekranında altyapı ve platform seviyesindeki servislerin telemetri verileri toplanmakta, analiz edilmekte ve gösterilmektedir.



Şekil 3. Uygulama izinlerinin alınması, saklanması ve okunması için kullanılan mimari



Şekil 4. Uygulama izinlerinin alınması, saklanması ve okunması için kullanılan mimari

3.5. Platform Servis İzleme

Platform servis izleme ekranında, kullanılan farklı teknoloji ve servisler için açık kaynak veya kurumsal telemetri verileri toplanmakta, analiz edilmekte ve gösterilmektedir. Servis İzleme Panosu Şekil 6'da gösterilmektedir.

3.6. Sürekli Profilleme

Sürekli profilleme ekranında uygulama kodunun profilinin çıkarılması hedeflenmiş ve bu sayede kaynak ve zaman açısından en yoğun olan kod bloklarının tespit edilerek hızlı aksiyon alınması sağlanmıştır.

3.7. Görselleştirme ve Raporlama Kullanıcı Arayüzü

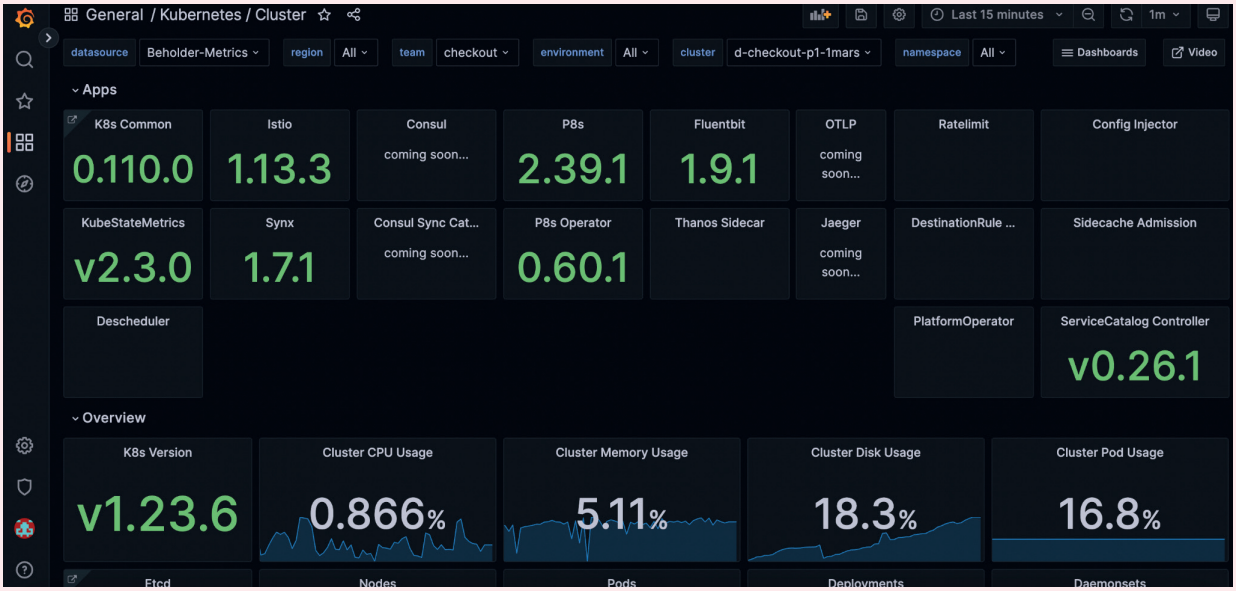
Görselleştirme ve Raporlama Kullanıcı Arayüzü ekranında büyük verinin görselleştirilmesi için kullanıcı ve servis bazlı özelleştirilebilen bir arayüz geliştirilmiştir. Bu arayüz sayesinde her ekip, servis sağlıklarını kontrol edebilmekte, geçmiş verileri tutabilmekte, özelleştirilmiş konfigürasyonlar yapabilmekte, özelleştirilmiş raporları ve grafikleri görüntüleyebilmekte ve alarmlar oluşturabilmektedir.

3.8. Alarm Oluşturma ve Raporlama

Alarm Oluşturma ve Raporlama ekranında metrik verilerinde tanımlanan alarm seviyeleri izlenebilmekte ve kullanıcılar özelleştirilmiş alarmlar oluşturulabilmektedir.

3.9. Akıllı Anomali Tespiti

Anomali tespiti, bir sistem, veri seti veya süreç içinde beklenen normal davranıştan sapmaları belirlemek için kullanılan bir tekniktir. Potansiyel sorunları erken aşamada belirlemesi ve çözmesi sebebiyle kritik bir öneme sahiptir. Bu bağlamda, akıllı anomali tespiti ekranında makine öğrenimi algoritmaları kullanılarak anomali tespit modelleri geliştirilmiştir. Bu modeller arasında istatistik tabanlı Otoregresif Entegre Hareketli Ortalama ve Mevsimsel Otoregresif Entegre Hareketli Ortalama gibi zaman serisi



Şekil 5. Altyapı İzleme Panosu

Şekil 6. Servis İzleme Panosu

tahminleme algoritmaları bulunmaktadır. Ayrıca, Tekrarlayan Sinir Ağı ve Geçitli Tekrarlayan Birim gibi derin öğrenme modelleri de yer almaktadır. İstatistiksel Anomali İzleme Panosu, Şekil 7'de gösterilmektedir.

3.10. Kök ve Etki Analizi

Kök ve etki analizi ekranında altyapıdaki tüm katmanların verileri tek bir platformda değerlendirilerek daha etkin, bütüncül ve hızlı bir şekilde kök neden ve potansiyel etki analizi yapılabilmesi sağlanmıştır.

3.11. Akıllı Kök Neden Analizi

Akıllı kök neden analizi ekranında geçmiş veriler kullanılarak kök nedenlerinin makine öğrenimi algoritmalarıyla modellemesi hedeflenmiştir. Bu modeller sayesinde yeni oluşan veya potansiyel senaryoların olası kök nedenleri akıllı sistemlerle otomatik olarak tespit edilebilmektedir.

3.12. Kullanıcı İzleme

Kullanıcı izleme ekranında uygulamanın işlevselliği ve performansının son kullanıcı deneyimine etkisi izlenmekte, raporlanmakta ve bu deneyimi etkileyen sistemdeki problemler ilgili ekiplerle paylaşılarak aksiyon alınmaktadır.

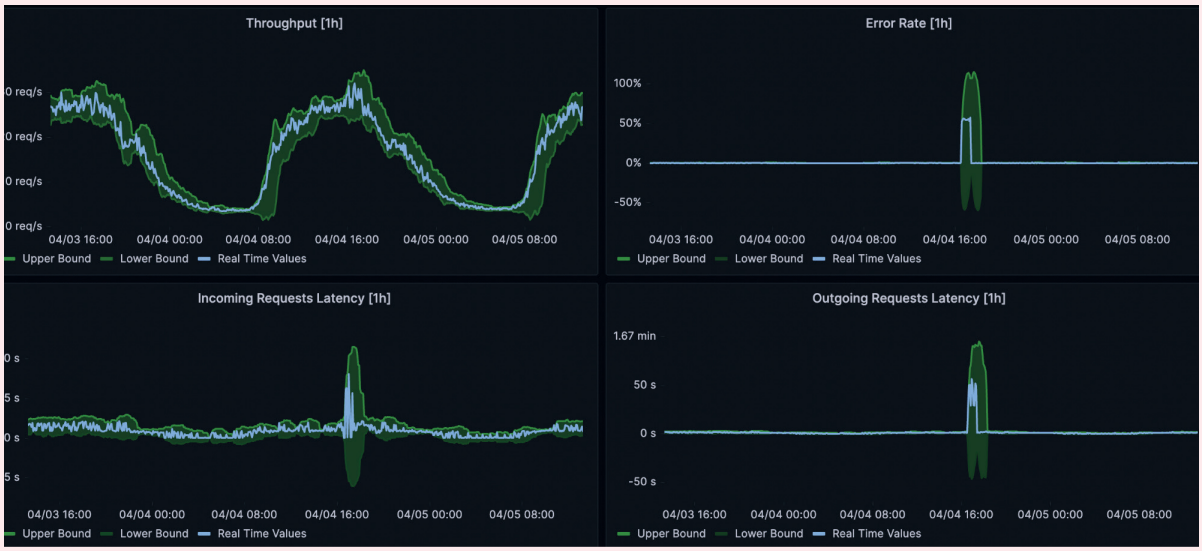
3.13. Yapay İzleme

Yapay izleme ekranında uygulama fonksiyonlarının yapay kullanıcılar aracılığıyla belirli aralıklarla test edilerek işlevselliği ve performansı simüle edilmekte ve potansiyel sorunların önleyici olarak tespiti ve aksiyon alınması sağlanmaktadır. Yapay İzleme Panosu Şekil 8'de gösterilmektedir.

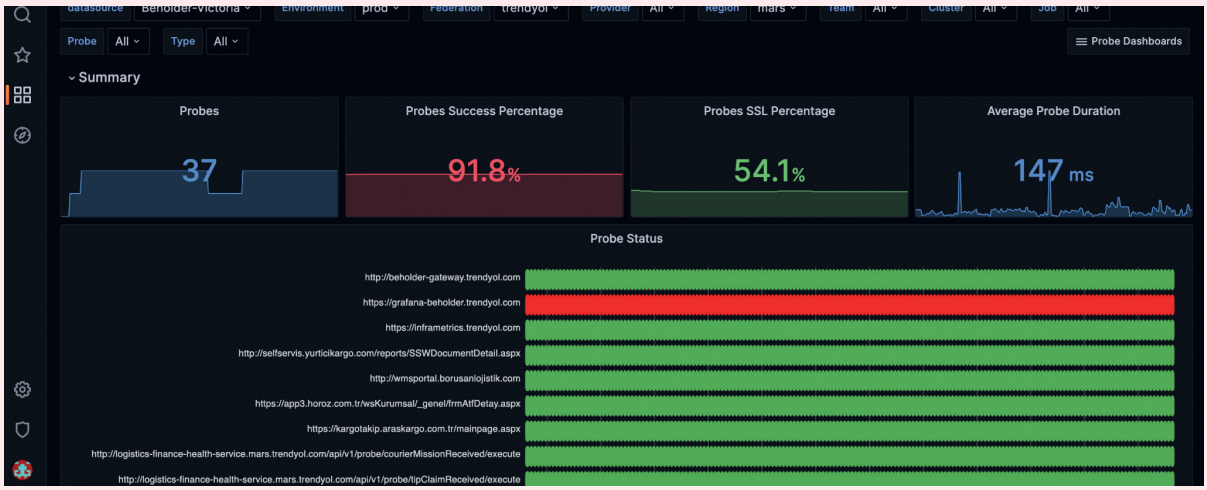
4. Çalışmanın Sonuçları

Geliştirilen platform ile,

- Alternatif tedarikçilere ödenen lisans ücretleri %50 azaltılmıştır.
- Gözlenebilirlik platformu kullanıcı sayısı %30 artırılmıştır.



Şekil 7. İstatistiksel Anomali İzleme Panosu



Şekil 8. Yapay İzleme Panosu

- Gözlenebilirlik projelerinin devreye alım eforu %60 azaltılmıştır.
- Problem bildirimlerinin çözüm süreleri %20 hızlanmıştır.
- Problem bildirim sayısı %10 azalmıştır.
- Hatalı problem bildirimleri %20 azalmıştır.
- Kesinti süreleri %20 azaltılmıştır.
- Son kullanıcı problem bildirimlerinin çözüm süreleri %10 hızlanmıştır.
- Net Promosyoncu Puanı (NPP), müşterilerin sadakatini ve memnuniyetini ölçmek için kullanılan bir metriktir. İşletmelerin büyüme ve gelişme stratejilerini şekillendirmede önemli bir yere sahiptir. Kullanıcı memnuniyetini ve sadakatini ölçmek amacıyla kullanılan bir metrik olan NPP, %50 iyileştirilmiştir.

5. Sonuç

Uygulama, altyapı ve ağ gözlenebilirliği yazılım uygulamaları, bilgi teknolojileri altyapılarını ve ağların performansını ve sağlığını izleme ve analiz etme sürecidir. Kullanıcılara daha verimli bir gözlenebilirlik deneyimi sunabilmek için web servisleri, kullanıcı arayüzleri ve akıllı analiz araçları geliştirilmiştir. Bu araçlar, kullanıcıların sistemde meydana gelen olayları anlık olarak takip etmelerini, potansiyel sorunları erken tespit edebilmelerini ve gerekli aksiyonları hızlı bir şekilde almalarını sağlamaktadır. Bu bağlamda, sistemlerde meydana gelen arızaların kök nedenlerini tespit etmek ve bu sorunların tekrarlanmaması için alınacak önlemler büyük önem taşımaktadır. Bu çalışmada, geçmiş veriyi inceleme, güvenlik, özelleştirme ve ölçeklenebilme gibi ihtiyaçlara yönelik bir platform geliştirilmiştir. Geliştirilen platform, ödenen lisans ücretlerinde %50 oranında maliyet tasarrufu sağlamıştır.

Orcid

Oğuzhan Demir https://orcid.org/0009-0007-1985-2210
Ahmet Can Uğur https://orcid.org/0009-0001-4911-5461
Mehmet Burak Deveci https://orcid.org/0009-0004-6100-0511
Mehmet Fatih Akay https://orcid.org/0000-0003-0780-0679
Ceren Ulus https://orcid.org/0000-0003-2086-6381

Referanslar

Alimohammadi, H., Chen, S. N. (2022). Performance Evaluation Of Outlier Detection Techniques İn Production Timeseries: A Systematic Review And Meta-Analysis. *Expert Systems With Applications*, *191*: 116371.

Bahri, M., Salutari, F., Putina, A., Sozio, M. (2022). Automl: State Of The Art With A Focus On Anomaly Detection, Challenges, And Research Directions. *International Journal Of Data Science And Analytics*, *14(2)*: 113-126.

Elsner, D., Aleatrati Khosroshahi, P., Maccormack, A. D., Lagerström, R. (2019). Multivariate Unsupervised Machine Learning For Anomaly Detection İn Enterprise Applications. In *Proceedings Of The 52nd Hawaii International Conference On System Sciences*, Jan 1, 2019, Bildiriler Kitabı, Pp. 5827-5836.

Emamjome, F., Andrews, R., Ter Hofstede, A., Reijers, H. (2020). Alohomora: Unlocking Data Quality Causes Through Event Log Context. In *Proceedings Of The 28th European Conference On Information Systems*, Jun 15 - 17, 2020, Bildiriler Kitabı, Pp. 1-16.

Gomez Blanco, D. (2023). Adopting Observability. In *Practical Open-Telemetry: Adopting Open Observability Standards Across Your Organization*, CA, Berkeley, pp. 217-229.

Hagemann, T., Katsarou, K. (2020). Reconstruction-Based Anomaly Detection For The Cloud: A Comparison On The Yahoo! Webscope S5 Dataset. In *Proceedings Of The 2020 4th International Conference On Cloud And Big Data Computing*, Aug 26 - 28, 2020, Birleşik Krallık, Bildiriler Kitabı, Pp. 68-75.

Hashemnia, N., Fan, Y., Rocha, N. (2021). Using Machine Learning To Predict And Avoid Malfunctions: A Revolutionary Concept For Condition-Based Asset Performance Management (Apm). In *2021 IEEE PES Innovative Smart Grid Technologies-Asia*, Dec 5 - 8, 2021, Brisbane, Avustralya, Bildiriler Kitabı, Pp. 1-8.

Khaled, A. S., Sharma, D. K., Yashwanth, T., Reddy, V. M. K., Doewes, R. I., Naved, M. (2022). Evaluating The Role Of Robotics, Machine Learning And Artificial Intelligence İn The Field Of Performance Management. In *Proceedings Of Second International Conference İn Mechanical And Energy Technology*, 2021, India, Bildiriler Kitabı, Pp. 285-293.

Manchanda, S. (2021). Artificial Intelligence Driven Monitoring, Prediction And Recommendation System (AIM-PRISM). In *Intelligent Sustainable Systems: Selected Papers Of Worlds4 2021*, Dec 17, 2021, Bildiriler Kitabı, Pp. 409-421.

O'Leary, C., Toosi, F. G., & Lynch, C. (2023). A Review of AutoML Software Tools for Time Series Forecasting and Anomaly Detection. *ICAART*, (3): 421-433.

Onodueze, F., Josyula, D. (2020). Anomaly Detection On MIL-STD-1553 Dataset Using Machine Learning Algorithms. In *2020 IEEE 19th International Conference On Trust, Security And Privacy İn Computing And Communications*, Dec 29 – Jan 1, 2021, Guangzhou, Çin, Bildiriler Kitabı, Pp. 592-598.

Ozer, G., Netti, A., Tafani, D., Schulz, M. (2020). Characterizing HPC Performance Variation With Monitoring And Unsupervised Learning. In *High Performance Computing: ISC High Performance 2020 International Workshops*, Jun 21–25, 2020, Frankfurt, Germany, Bildiriler Kitabı, Pp. 280-292.

Pintilie, I., Manolache, A., Brad, F. (2023). Time Series Anomaly Detection Using Diffusion-Based Models. In *2023 IEEE International Conference On Data Mining Workshops*, Aralık 4, 2023, Şanghay, Çin, Bildiriler Kitabı, Pp. 570-578.

Princz, G., Shaloo, M., & Erol, S. (2024). Anomaly Detection in Binary Time Series Data: An unsupervised Machine Learning Approach for Condition Monitoring. *Procedia Computer Science*, 232:

1065-1078.

Qiu, J., Du, Q., Qian, C. (2019). Kpi-Tsad: A Time-Series Anomaly Detector For Kpi Monitoring İn Cloud Applications. *Symmetry*, *11*(11): 1350.

Tang, Y., Wang, H., Zhan, X., Luo, X., Zhou, Y., Zhou, H., Keung, J. (2021). A Systematical Study On Application Performance Management Libraries For Apps. *IEEE Transactions On Software Engineering*, *48*(8): 3044-3065.

Zhou, X., Peng, X., Xie, T., Sun, J., Ji, C., Liu, D., He, C. (2019). Latent Error Prediction And Fault Localization For Microservice Applications By Learning From System Trace Logs. In *Proceedings Of The 2019 27th ACM Joint Meeting On European Software Engineering Conference And Symposium On The Foundations Of Software Engineering*, Aug 26 - 30, 2019, Tallin, Estonya, Bildiriler Kitabı, Pp. 683-694.