

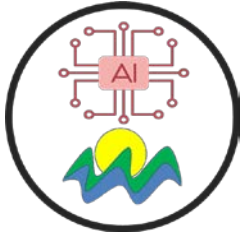
Black Sea Journal of Artificial Intelligence

Volume 1 | Issue 1



ISSN: 3108-4281


KAR-YAY



BLACK SEA JOURNAL OF ARTIFICIAL INTELLIGENCE
(BSJ AI)



Black Sea Journal of Artificial Intelligence (BSJ AI) is an international a peer-reviewed journal published electronically twice a year in June and December. BSJ AI publishes original research, innovative methodologies, and interdisciplinary studies in the fields of artificial intelligence. The journal provides a global platform for researchers, scientists, engineers, and practitioners to address contemporary and emerging artificial intelligence challenges and to develop sustainable solutions for artificial intelligence. BSJ AI is published electronically and all articles are provided to the readers free of charge.

e-ISSN: 3108-4281

Phone: +90 362 408 25 15

Fax: +90 362 408 25 15

Email: bsjai@blackseapublishers.com

Web site: <https://blackseapublishers.online/index.php/ai>

Sort of publication: Periodically 2 times (June and December) in a year

Publication date and place: June 15, 2025- Samsun, TÜRKİYE

Publishing kind: Electronically

OWNER

KARYAY Karadeniz Yayımcılık ve Organizasyon Ticaret Limited Company

DIRECTOR IN CHARGE

Prof. Dr. Hasan ÖNDER

EDITOR BOARDS

EDITOR IN CHIEF

Prof. Dr. Mehmet Serhat ODABAŞ, Ondokuz Mayıs University, TÜRKİYE

SECTION EDITORS*

Assoc. Prof. Dr. Cem TIRINK, Iğdır University, TÜRKİYE

Assoc. Prof. Dr. Thobela Louis TYASI, University of Limpopo, SOUTH AFRICA

Dr. Alper GÜLBE, Iğdır University, TÜRKİYE

Dr. Hakan Can ALTUNAY, Ondokuz Mayıs University, TÜRKİYE

* The ranking is arranged alphabetically within the academic title

STATISTIC EDITOR

Prof. Dr. Mehmet TOPAL, Kastamonu University, TÜRKİYE

ENGLISH EDITOR

Assist. Prof. Dr. Betül ÖZCAN DOST, Ondokuz Mayıs University, TÜRKİYE

TURKISH EDITOR

Prof. Dr. Serkan ŞEN, Ondokuz Mayıs University, TÜRKİYE

REVIEWERS OF THE ISSUE*

Prof. Dr. Hasan ÖNDER, Ondokuz Mayıs University, Department of Animal Science, Machine Learning Algorithms, TÜRKİYE

Assist. Prof. Dr. Emre ENGİN, Ondokuz Mayıs University, Department of Computer Technologies, Artificial Intelligence, TÜRKİYE

Assist. Prof. Dr. Esra YAVUZ, Şırnak University, Department of Accounting and Tax, Artificial Intelligence, TÜRKİYE

Assist. Prof. Dr. Hacer Kübra SEVİNÇ, Karabük University, Department of Software Application Development and Analysis, Machine Learning Algorithms, TÜRKİYE

Assist. Prof. Dr. Mustafa MUTLU, Ordu University, Department of Electronics and Automation, Artificial Intelligence, TÜRKİYE

Assist. Prof. Dr. Ömer Faruk ACAR, Karabük University, Department of Software Engineering, Artificial Intelligence, TÜRKİYE

Dr. Hasan Alp ŞAHİN, Ondokuz Mayıs University, Hemp Research Institute, Artificial Intelligence, TÜRKİYE

Dr. Murat VAROL, Zonguldak Bülent Ecevit University, Department of Computer Engineering, Artificial Intelligence, TÜRKİYE

* The ranking is arranged alphabetically within the academic title

Table of Contents

Research Articles

1. BİLGİYE ERİŞİMDE YENİ UFUKLAR: DİJİTAL KÜTÜPHANE VE YAPAY ZEKÂ LİTERATÜRÜNÜN BİBLİYOMETRİK HARİTASI

Engin DAYAN.....1-10

2. PHISHING ATAKLARININ BÜYÜK DİL MODELLERİ ÜZERİNE ETKİLERİ

Hakan Can ALTUNAY.....11-14

3. JAVASCRIPT FONKSİYONLARINDA GÜVENLİK AÇIKLARININ MAKİNE ÖĞRENMESİ YÖNTEMLERİYLE TESPİTİ

Hasan Hüseyin ALAV, Özgür TONKAL, Zafer CÖMERT.....15-24

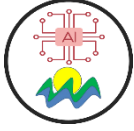
Reviews

4. VERİ OKURYAZARLIĞINDAN YAPAY ZEKÂYA: DİJİTAL ÇAĞIN ELEŞTİREL YETKİNLİKLERİ ÜZERİNE BİR DERLEME

Engin DAYAN.....25-30

5. YAPAY ZEKA ÇAĞINDA BİLGİSAYAR AĞLARI YÖNETİMİ VE GÜVENLİĞİ

Serkan VARAN.....31-34



BİLGİYE ERİŞİMDE YENİ UFUKLAR: DİJİTAL KÜTÜPHANE VE YAPAY ZEKÂ LİTERATÜRÜNÜN BİBLİYOMETRİK HARİTASI

Engin DAYAN^{1*}

¹Iğdır University, Vocational School of Health Services, 76200, Iğdır, Türkiye

Özet: Dijital kütüphaneler ile yapay zekânın (AI) kesişimi, bilgiye erişim alanını köklü bir şekilde dönüştürerek bilgi keşfi ve paylaşımı için benzersiz fırsatlar sunmuştur. Bu çalışma, dijital kütüphaneler ve yapay zekâ literatürünün kesişiminde yer alan yayınları kapsamlı bir bibliyometrik analizle incelemekte olup, Web of Science veri tabanından elde edilen verileri kullanmaktadır. Yayın eğilim analizi, anahtar kelime bulutu oluşturma, anahtar kelimelerin tematik analizi, anahtar kelimelerin birlikte görülme analizi ve trend kavram analizi gibi bibliyometrik teknikler uygulanarak, bu alandaki entelektüel yapı, baskın temalar ve yeni ortaya çıkan eğilimler haritalandırılmıştır. Bulgular, dijital kütüphanelerde yapay zekâ destekli uygulamaların, örneğin akıllı arama sistemleri, otomatik meta veri çıkarımı ve kişiselleştirilmiş öneri motorlarının hızla arttığını ortaya koymaktadır. Bununla birlikte, veri gizliliği, algoritmik önyargı ve teknolojik altyapı eşitsizlikleri gibi zorluklar da tespit edilmiştir. Analiz, temel araştırma kümelerini, etkili yayınları ve disiplinlerarası bağlantıları ortaya koyarak küresel araştırma manzarasına dair kapsamlı bir bakış sunmaktadır. Yapay zekânın dijital kütüphane sistemlerindeki evrimini ve etkisini aydınlatarak, bu bibliyometrik harita, araştırma boşluklarına ve gelecekteki yönelimlere dair değerli içgörüler sağlamakta; kapsayıcı ve verimli bilgi ekosistemlerinin geliştirilmesi için bir temel oluşturmaktadır.

Anahtar kelimeler: Dijital kütüphaneler, Yapay zekâ, Bibliyometrik analiz, Bilgiye erişim

New Horizons in Information Access: Bibliometric Mapping of Digital Libraries and Artificial Intelligence Literature

Abstract: The convergence of digital libraries and artificial intelligence (AI) has significantly reshaped information access, fostering innovative approaches to knowledge discovery and dissemination. This study conducts a comprehensive bibliometric analysis of the literature at the intersection of digital libraries and AI, utilizing data from the Web of Science database. Employing a suite of bibliometric techniques—including publication trend analysis, keyword cloud generation, thematic analysis of keywords, co-occurrence analysis of keywords, and trend concept analysis—this research maps the intellectual structure, dominant themes, and emerging trends in the field. The findings highlight a surge in AI-driven applications within digital libraries, such as intelligent search systems, automated metadata extraction, and personalized recommendation engines, while also identifying challenges such as data privacy, algorithmic bias, and disparities in technological infrastructure. The analysis reveals key research clusters, influential publications, and interdisciplinary connections, providing a robust overview of the global research landscape. By elucidating the evolution and impact of AI in digital library systems, this bibliometric map offers valuable insights into research gaps and future directions, serving as a foundation for advancing inclusive and efficient knowledge ecosystems.

Keywords: Digital libraries, Artificial intelligence, Bibliometric analysis, Information access

*Sorumlu yazar (Corresponding author): Iğdır University, Vocational School of Health Services, 76200, Iğdır, Türkiye

E mail: engin.dayan065@gmail.com (E. DAYAN)

Engin DAYAN <https://orcid.org/0000-0003-1839-280X>

Gönderi: 10 Mayıs 2025

Kabul: 23 Mayıs 2025

Yayınlanma: 15 Haziran 2025

Received: May 10, 2025

Accepted: May 23, 2025

Published: June 15, 2025

Cite as: Dayan, E. (2025). New horizons in information access: Bibliometric mapping of digital libraries and artificial intelligence literature. *Black Sea Journal of Artificial Intelligence*, 1(1), 1-10.

1. Giriş

21. yüzyılda yapay zekâ (YZ) teknolojilerindeki hızlı ilerlemeler, bilgiye erişim, yönetim ve paylaşım süreçlerini dönüştürerek dijital kütüphaneleri daha akıllı, erişilebilir ve kullanıcı odaklı sistemlere evrilmiştir. YZ destekli dijital kütüphaneler, akıllı arama motorları, otomatik meta veri çıkarımı, metin madenciliği, kişiselleştirilmiş öneri sistemleri ve içerik analitiği gibi yenilikçi uygulamalarla bilgi hizmetlerinin niteliğini yeniden tanımlamaktadır. Bu teknolojiler, bilgi keşfi ve kullanıcı deneyimini iyileştirirken, kütüphane bilimi ile bilgisayar mühendisliği arasındaki disiplinlerarası

etkileşimi güçlendirmektedir.

Bununla birlikte, YZ'nin dijital kütüphanelere entegrasyonu yalnızca teknik avantajlar sunmakla kalmamakta; veri gizliliği, algoritmik önyargı, hesap verebilirlik ve bilgiye adil erişim gibi etik ve toplumsal sorunları da gündeme getirmektedir. Kullanıcı davranışlarının izlenmesi, kişisel verilerin işlenmesi ve içerik filtreleme mekanizmaları, bu alanda daha derinlemesine etik değerlendirmeleri ve düzenleyici çerçeveleri zorunlu kılmaktadır. Mevcut literatür, YZ ve dijital kütüphanelerin kesişimine dair çeşitli çalışmalar sunmakla birlikte, bu alandaki yayınların kapsamlı bir



bibliyometrik analizi henüz yeterince gerçekleştirilmemiştir. Bu eksiklik, araştırma eğilimlerini, tematik odakları ve iş birliği ağlarını sistematik bir şekilde haritalandırma ihtiyacını ortaya koymaktadır.

Bu çalışma, YZ ve dijital kütüphane literatürünün kesişiminde yer alan akademik yayınları Web of Science veri tabanından elde edilen verilerle bibliyometrik yöntemler aracılığıyla analiz etmeyi amaçlamaktadır. Yayın eğilim analizi, anahtar kelime bulutu, anahtar kelimelerin tematik ve birlikte görülme analizleri ile trend kavram analizi gibi yöntemler kullanılarak, alandaki entelektüel yapı, etkili yayınlar, iş birliği ağları ve baskın temalar ortaya konulacaktır. Çalışma, YZ'nin dijital bilgi yönetimi, kullanıcı deneyimi, otomatik kataloglama, bilgi güvenliği ve içerik analitiği gibi alt alanlardaki etkilerini değerlendirerek, bu teknolojilerin kütüphane bilimi, bilgi etiği ve bilgi okuryazarlığı üzerindeki dönüştürücü rolünü bütüncül bir perspektifle incelemeyi hedeflemektedir. Bu bağlamda, analiz, araştırmacılar, kütüphaneciler ve politika yapıcılar için bilgi toplumunda YZ destekli dijital kütüphanelerin geleceğine dair stratejik içgörüler sunmayı ve alandaki araştırma boşluklarını dolduracak bir yol haritası önermeyi amaçlamaktadır. Araştırma soruları şunlardır:

- Kütüphanecilikte Yapay Zekâ 'ya ilişkin literatürde yayın ve atıf eğilimleri nelerdir?
- Bu alanda öne çıkan ülkeler ve yayıncılar hangileridir?
- Kütüphanecilikte Yapay Zekâ üzerine araştırma yayınlamak için en iyi kaynaklar (dergiler) hangileridir?
- Literatürdeki yazarlık ve anahtar kelime birlikteliği kalıplarına bakıldığında, Yapay Zekâ araştırmalarının kütüphaneciliğe sağladığı temel fikirler ve katkılar nelerdir?
- Ülkeler arası iş birliği, kütüphanecilikte Yapay Zekâ alanında bilginin nasıl yaratılıp paylaşıldığını nasıl etkiliyor?

2. Literatür

Yapay zekâ (YZ) teknolojilerinin dijital kütüphanelere entegrasyonu, bilgiye erişim, yönetim ve paylaşım süreçlerinde köklü bir dönüşüm yaratmıştır. Bu kesişim, kütüphane bilimi ile bilgi teknolojileri arasında disiplinlerarası bir sinerji oluşturarak akıllı arama sistemleri, otomatik meta veri çıkarımı, kişiselleştirilmiş öneri motorları ve içerik analitiği gibi yenilikçi uygulamaları mümkün kılmıştır (Vasishta vd., 2025). Bibliyometrik analiz, bu dinamik alanın entelektüel yapısını, yayın eğilimlerini ve tematik evrimini haritalandırmak için etkili bir yöntem olarak öne çıkmaktadır (Bornmann ve Mutz, 2015).

Son yıllarda, dijital kütüphanelerdeki büyük veri uygulamaları ve buna ilişkin bibliyometrik çözümleme yöntemleri, literatürde hızla önem kazanmıştır. Bibliyometrik teknikler, özellikle kütüphane ve bilgi

bilimi alanındaki araştırma yönelimlerini, sıcak konuları ve atıf ağlarını ortaya koymada sıklıkla kullanılmaktadır (Ellegaard ve Wallin, 2015; Alam vd., 2023). Bu yöntemler, sadece yayın hacmini değil; aynı zamanda bilimsel etkileri, ortaklık yapıları ve bilgi alanının tematik gelişimini de analiz etme olanağı sunar.

Geniş çaplı veri kümeleriyle birlikte, YZ ve büyük veri teknolojileri arasındaki etkileşim dijital kütüphanelerin altyapısını da yeniden şekillendirmektedir. Cox ve Mazumdar (2024) göre, YZ teknolojilerinin yükselişi, büyük verinin işlenmesiyle doğrudan bağlantılıdır. Büyük veri analitiği, yalnızca içerik yönetimini iyileştirmekle kalmaz, aynı zamanda kullanıcı davranışlarını anlamaya, hizmetleri kişiselleştirmeye ve bilgiye erişimi optimize etmeye de olanak tanır (Wijewickrema, 2023). Bu bağlamda kütüphaneler, geleneksel hizmet yapılarından çıkarak, veri merkezli bir bilgi erişim paradigmasına doğru evrilmektedir.

Bu dönüşümde teknik kütüphanecilik becerileri, veri analitiği, algoritmik okuryazarlık ve dijital etik gibi alanlarla bütünleşmektedir (Johnson, 2017). Kim ve Cooke (2017), kamu kütüphanesi hizmetleri için gerçekleştirdikleri büyük veri analizinde, veri doğruluğu, güvenliği ve sıkıştırma gibi temel sorunları tanımlamış; Chernoff yüz yaklaşımıyla hizmet kalitesini görselleştirmede yeni bir yöntem ortaya koymuşlardır. Campbell ve Cowan (2016) ise, bağlantılı veri teknolojilerinin kullanıcıların kendi kendine öğrenme süreçlerini desteklediğini ve büyük veri yaklaşımlarından daha etkin sonuçlar doğurduğunu belirtmiştir.

YZ'nin kütüphanelerdeki pratik uygulamalarına dair literatür de çeşitlenmektedir. Sohbet robotları (chatbot), veri madenciliği, dijital içerik öneri sistemleri ve akıllı kataloglama araçları, modern kütüphanelerin kullanıcıya dönük yüzünü belirleyen temel teknolojiler haline gelmiştir (Allison, 2012). Bunun yanında, sosyal medya verilerinin analizi de dijital kütüphane uygulamalarına entegre edilmiştir. YouTube ve WeChat gibi platformlar, kişiselleştirilmiş içerik sunumu ve hizmet değerlendirme araçları olarak kullanılmakta; bu sayede kullanıcı etkileşimi daha ölçülebilir hale gelmektedir (Zhang ve Lu, 2023; Deori vd., 2023).

COVID-19 pandemisi, dijitalleşme eğilimlerini hızlandırmış ve büyük veri uygulamalarını kaçınılmaz kılmıştır. Kütüphaneler, bu dönemde hem operasyonel adaptasyonlar hem de kullanıcı davranışı analizleri için büyük veri analitiklerinden faydalanmışlardır (Yu vd., 2022). Bu süreçte bilgi davranışı, sanal öğrenme entegrasyonları ve uzaktan hizmet tasarımı gibi konular ön plana çıkmıştır (Meng vd., 2023). Ayrıca sosyal robotlar, artırılmış gerçeklik gibi teknolojiler aracılığıyla kullanıcı deneyiminin zenginleştirilmesi hedeflenmiştir (Tung ve Jara Santiago Campos, 2022).

Mevcut literatürde, YZ ile dijital kütüphanelerin kesişiminde dikkat çeken bazı sınırlılıklar göze çarpmaktadır. Çoğu çalışma belirli uygulamalara odaklanmakta ve alanın bütüncül haritasını sunmakta yetersiz kalmaktadır (Hervieux ve Wheatley, 2021).

Ayrıca, veri gizliliği, algoritmik önyargı, dijital eşitsizlik ve çoklu veri kaynaklarının karşılaştırmalı kullanımı gibi konular hâlâ yeterince ele alınmamıştır (Alemneh vd., 2019). Coğrafi temsildeki dengesizlikler ve yalnızca tek bir veri tabanına dayanan çalışmalar da metodolojik açıdan sınırlayıcı olmaktadır.

Bu çalışma, belirtilen literatür boşluklarını gidermek amacıyla, Web of Science veri tabanındaki yayınlara dayalı kapsamlı bir bibliyometrik analiz sunmaktadır. Yayın trendleri, yazar işbirliği ağları, anahtar kelime birlikte görülme haritaları ve tematik kümeler aracılığıyla, YZ ve dijital kütüphane etkileşiminin akademik evrimi sistematik olarak haritalandırılacaktır. Böylece, hem araştırmacılar hem de uygulayıcılar için stratejik yönelimler, araştırma fırsatları ve bilgi altyapılarının gelişimi açısından değerli içgörüler elde edilmesi hedeflenmektedir. Ayrıca, kütüphanelerdeki yapay zekâ uygulamalarıyla ilgilenen kütüphaneciler, bilgi bilimcileri ve diğer araştırmacılar için yararlı olacağı umulmaktadır.

3. Materyal ve Yöntem

3.1. Yöntem

Kütüphanecilikte yapay zekâ uygulamalarının araştırma ve yayın desenlerini analiz etmek için bibliyometrik yöntem uygulandı. Bibliyometrik analiz öncelikle belirli disiplinler içindeki araştırma konularını ve bunların birbirleriyle olan bağlantılarını ortaya çıkarmayı ve incelemeyi amaçlamaktadır (Önder, 2025). Tijjani vd. (2021) ve Guleria ve Kaur (2021) bibliyometrik yöntemin akademik yayın modellerini görselleştirmek için yerleşik bir nicel yöntem olduğunu belirtmiştir. Ayrıca, bibliyometrik, dünya çapında bilimsel literatüre katkıda bulunan yazarların, ülkelerin, kuruluşların ve işbirliklerinin bilimsel bir manzarasını sunar (Islam vd., 2022).

3.2. Veritabanı Seçimi

Diğer benzer çalışmalara uygun olarak (Huo vd., 2015; Martín-Del-Río vd., 2018), bu çalışmayı yürütmek için Web of Science (WOS) platformu kullanıldı. WOS araştırma motoru, çok disiplinli yapısı nedeniyle bilimsel aktiviteyi analiz eden çalışmalarda yaygın olarak kullanılır. Dünya çapında 150'den fazla disipline karşılık gelen 12.000'den fazla dergi dâhil olmak üzere tüm bilimsel ve teknolojik alanları kapsar ve oluşturulan atıflar ve tüm kurumların adresleri hakkında bilgi içerir (Moed, 2009).

Özellikle, bu çalışma için makaleler Web of Science (WOS) platformu aracılığıyla danışılan beş veritabanından çıkarıldı: Web of Science Core Collection, Current Contents Connect, Medline, SciELO Citation Index ve Korean Journal Database.

3.3. Arama Sorgusu

Maksimum çalışma sayısını belirlemek için başlıktaki veya özetindeki tüm terimler arandı. Arama denklemi şu şekildeydi: (Dijital kütüphane [Başlık VEYA Özet] VEYA Dijital kütüphaneler [Başlık VEYA Özet] VEYA Çevrim içi kütüphane [Başlık VEYA Özet] VEYA Kurumsal depo

[Başlık VEYA Özet]) VE (Yapay zekâ [Başlık VEYA Özet] VEYA Makine öğrenmesi [Başlık VEYA Özet] VEYA Derin öğrenme [Başlık VEYA Özet]) VE (Bibliyometrik analiz [Başlık VEYA Özet] VEYA Bilimsel ölçüm analizi [Başlık VEYA Özet]). Mektuplar, kitaplar, biyografiler, referans materyalleri, özetler, toplantılar ve haberler veya düzeltmeler hariç olmak üzere yalnızca belge türü filtresi uygulandı.

3.4. Dâhil Etme ve Hariç Tutma Ölçütleri

Bu çalışma, yapay zekâ (YZ) ve dijital kütüphanelerin kesişiminde yer alan akademik yayınların bibliyometrik analizini gerçekleştirmek amacıyla Web of Science veri tabanından elde edilen verileri kullanmıştır. Maksimum çalışma sayısını belirlemek için, başlık veya özetlerde belirli terimleri hedefleyen bir arama denklemi oluşturulmuştur. Bu denklem ile YZ teknolojilerinin dijital kütüphanelerdeki uygulamalarını (örneğin, akıllı arama sistemleri, otomatik meta veri çıkarımı, kişiselleştirilmiş öneri motorları), bilgi erişimi ve yönetimi üzerindeki etkilerini veya veri gizliliği ve algoritmik önyargı gibi etik ve toplumsal sorunlara yönelik değerlendirmeleri ele alan yayınları kapsamayı amaçlamaktadır.

Dâhil etme kriterleri, yayınların yalnızca YZ ve dijital kütüphanelerin kesişimine odaklanmasını ve bibliyometrik analiz veya bilimsel ölçüm analizi yöntemlerini içermesini gerektirmiştir. Çalışma türü (örneğin, makale, derleme, konferans bildirisi) ve diline bakılmaksızın tüm yayınlar dâhil edilmiştir. Ancak, belge türü filtresi uygulanarak mektuplar, kitaplar, biyografiler, referans materyalleri, özetler, toplantılar ve haberler veya düzeltmeler hariç tutulmuştur. Bu filtre, analizin yalnızca akademik makaleler ve araştırma odaklı yayınlarla sınırlı kalmasını sağlamıştır.

Hariç tutma kriterleri, çalışmanın odak noktasını netleştirmek için şu şekilde tanımlanmıştır: YZ'nin dijital kütüphaneler dışındaki bilgi sistemlerinde (örneğin, sağlık, finans veya eğitim sektörleri) veya fiziksel kütüphane altyapılarına odaklanan yayınlar analiz kapsamı dışında bırakılmıştır. Ayrıca, YZ veya dijital kütüphanelerle ilgili ancak bibliyometrik analiz veya bilimsel ölçüm analizi içermeyen çalışmalar da hariç tutulmuştur. Bu kriterler, çalışmanın yalnızca YZ ve dijital kütüphanelerin kesişiminde bibliyometrik yöntemlerle yapılan araştırmalara odaklanmasını ve tutarlı bir veri seti oluşturulmasını sağlamayı hedeflemektedir.

Çalışmanın güvenilirliği için iki araştırmacı makaleleri bağımsız olarak değerlendirip, dâhil etme kriterlerini uygulamış; farklılıklar ortak görüşle çözülmüştür.

3.5. Bibliyometrik Göstergeler

Önerilen hedeflere ulaşmak için aşağıdaki üç tür bibliyometrik gösterge kullanıldı. Bilimsel üretkenlik göstergeleri: Yazarlar, kurumlar, dergiler, en üretken ülkeler, yayımlanmış belge türleri ve yayım dili analiz edildi. Etki göstergeleri: Alınan verilerin bilimsel etkisini değerlendirmek için kullanılan göstergeler alınan atıflar ve derginin dâhil edildiği temattaki dergi sıralamasıydı.

Bu veriler WOS'tan Science Citation Index Expanded (SCIE) ve Social Science Citation Index'ten (SSCI) elde edildi. İş birliği göstergeleri: Ortak atıf ağları analiz edildi ve yazarların anahtar kelimelerinin ortak oluşumu görselleştirildi.

3.6. Veri Analizi

WOS'tan alınan veriler yüzdeleri ve frekansları hesaplamak, şekilleri ve tabloları oluşturmak için Microsoft Excel yazılımı kullanıldı. Raporlar ve sorgular bibliyometrik göstergeleri analiz etmek ve küresel veriler elde etmek için oluşturuldu. Yazarlar, atıflar ve anahtar kelimeler hakkındaki veriler, bibliyometrik ağları ve görselleştirmeleri elde etmek için Rstudio yazılımı ile analiz edildi.

4. Bulgular

4.1. Yayınlarla İlişkin Temel Bilgiler

Arama stratejisi doğrultusunda, Web of Science veri tabanında toplam 356 kayıt elde edilmiştir. Belirlenen dahil etme ve hariç tutma kriterlerinin sistematik biçimde uygulanmasının ardından, analiz için 107 makale

seçilmiştir. Bu çalışmalar, 1995 ile 2025 yılları arasında yayımlanmış olup, doğrudan Yapay Zekâ (YZ) ve Dijital Kütüphane konularının kesişiminde yer alan araştırmaları kapsamaktadır.

Tablo 1'de sunulan bulgular, dijital kütüphane ve yapay zekâ alanındaki bilimsel yayınların kapsamını, yapısını ve gelişim eğilimlerini detaylı biçimde ortaya koymaktadır. Bibliyometrik analiz kapsamında toplam 107 doküman, 56 farklı kaynaktan elde edilmiştir. Yayınların tarih aralığı 1995–2025 yıllarını kapsamaktadır; bu da alanın yaklaşık 30 yıllık bir gelişim sürecine sahip olduğunu göstermektedir. Yayınların ortalama yaşı 4,58 yıl olup, bu durum konunun güncelliğini koruduğunu ortaya koymaktadır. Ayrıca, yayınların yıllık ortalama büyüme oranı %8,6 olarak hesaplanmış; bu da alana yönelik akademik ilgide istikrarlı bir artış olduğunu göstermektedir. Sonuç olarak, dijital kütüphanelerde yapay zekâ uygulamalarının öneminin giderek artmakta olduğunu ve disiplinlerarası araştırmaların bu alanda yoğunlaştığını ortaya koymaktadır.

Tablo 1. Temel bilgilere ait sonuçlar

Temel Bilgileri	Sonuçlar	%
Çeşitli Veriler		
Kaynak sayısı	56	--
Belge sayısı	107	--
Yayın aralığı	1995-2025	--
Yayınların ortalama yaşı	4,58	
Yayınların yıllık ortalama artış oranı	--	%8,6
Yazar Verileri		
Yazar sayısı	485	--
Tek yazarlı yayın sayısı	8	
Yazar İş Birliği Verileri		
Belge başına ortalama yazar sayısı	4,65	--
Uluslararası iş birliği oranı	--	30,8
Yayın İçeriği		
Yayınlarda kullanılan anahtar kelime sayısı	570	--
Yayınlarda atıf yapılan kaynak sayısı	8036	
Yayın Türü Verileri		
Araştırma makalesi	68	63,5
Derleme	39	36,4
Atıf Verileri		
Yayın başına ortalama atıf sayısı	19,0	--
En Aktif Beş Yazarın Ülkeleri		
ABD	75	70,0
Çin	48	44,8
Pakistan	31	28,9
İspanya	28	26,1
Hindistan	27	25,2
Alanın En Fazla Yayın Yapan Beş Dergisi		
IEEE Access	23	21,4
Digital Library Perspectives	7	6,5
Journal Of The American Medical Informatics Association	6	5,6
International Journal On Digital Libraries	5	4,6
Information	3	2,8

Toplamda 485 yazarın katkı sağladığı bu yayınlarda, yalnızca 8 makalenin tek yazarlı olduğu görülmektedir. Her bir makalede ortalama 4,65 yazar yer almakta, bu da dijital kütüphane ve yapay zekâ konularında çok yazarlı ve iş birliğine dayalı araştırma eğilimini açıkça ortaya koymaktadır. Uluslararası düzeyde iş birliği oranı da dikkat çekicidir: %30,8 oranında uluslararası ortak yazarlık tespit edilmiştir (Tablo 1). Bu oran, alanın küresel ölçekte araştırmacılar arasında nasıl paylaşıldığını ve geliştiğini göstermektedir.

Yayınlarda toplam 570 farklı anahtar kelime kullanılmış ve kaynakça olarak toplam 8036 farklı kaynak referans gösterilmiştir. Bu yoğun referans kullanımı, alanın teorik ve metodolojik zenginliğini yansıtmaktadır. Yayın türleri incelendiğinde, belgelerin %63,5'i (n=68) araştırma makalesi, %36,4'ü (n=39) ise derleme ya da sistematik derleme türündedir. Araştırma makalelerinin çoğunlukta olması, konunun yalnızca kuramsal değil, aynı zamanda uygulamalı yaklaşımlarla da ele alındığını ortaya koymaktadır (Tablo 1).

Her bir yayın için ortalama 19,0 atıf alınması, çalışmalara yönelik akademik görünürlüğün ve etkinin oldukça yüksek olduğunu göstermektedir. Bu bulgu, bilginin dijitalleşmesi ve yapay zekâyla yeniden yapılandırılmasının akademik topluluk tarafından yoğun şekilde takip edildiğini desteklemektedir (Tablo 1)

Ayrıca, en üretken beş ülke sırasıyla Amerika Birleşik Devletleri (75 makale, %70,0), Çin (48, %44,8), Pakistan (31, %28,9), İspanya (28, %26,1) ve Hindistan'dır (27, %25,2). Bu dağılım, dijital bilgi sistemleri ve yapay zekâ uygulamalarının özellikle gelişmiş ve gelişmekte olan ülkeler düzeyinde önemli bir araştırma konusu haline geldiğini göstermektedir (Tablo 1).

Yayınlara en sık yer aldığı beş dergi ise şu şekildedir:

- IEEE Access (23 yayın, %21,4),
- Digital Library Perspectives (7 yayın, %6,5),
- Journal of the American Medical Informatics Association (6 yayın, %5,6),
- International Journal on Digital Libraries (5 yayın, %4,6),
- Information (3 yayın, %2,8).

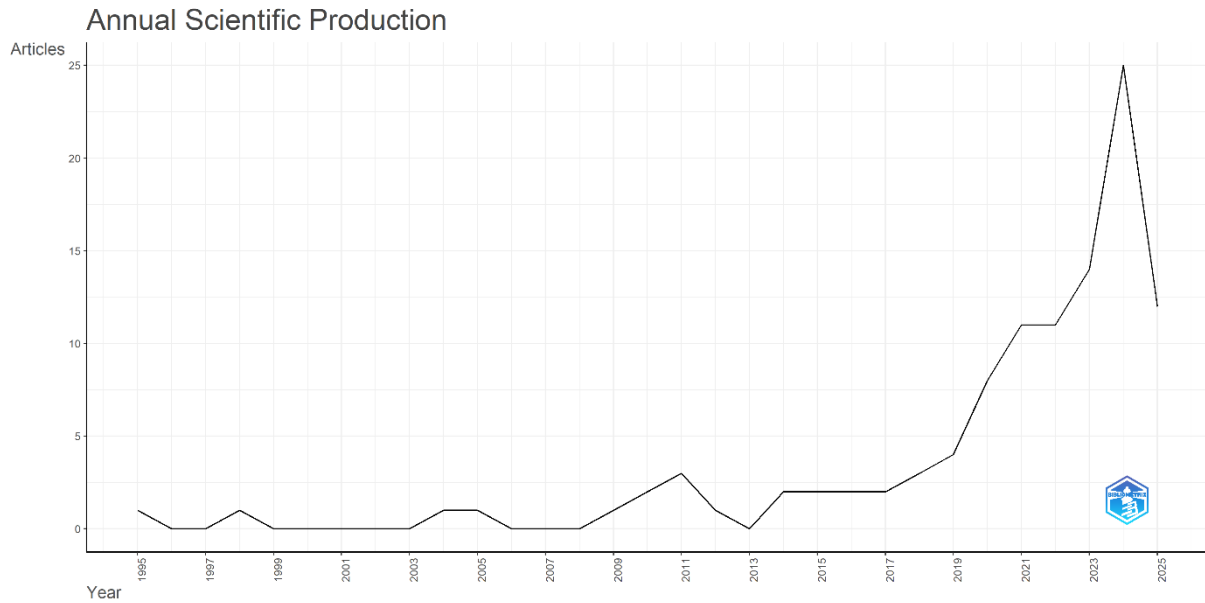
Bu dergilerin çoğu bilgi bilimi, dijital kütüphaneler ve yapay zekâ alanlarında uzmanlaşmış olup, çalışmanın tematik kapsamıyla doğrudan örtüşmektedir.

4.2. Yayınların Yıllara Göre Dağılımı

Yıllara göre dağılım incelendiğinde; yıllık yayın sayısında artış ve azalmalar görülmektedir. 1995–2025 yılları arasında yapay zekâ ve dijital kütüphaneler konularında yayımlanan akademik çalışmaların yıllık dağılımı, alanın gelişimini ortaya koymaktadır. 1995–2005 yılları arasında yayın sayısının oldukça düşük ve durağan olduğu görülmektedir (Şekil 1). Bu dönem, konunun henüz yeni yeni şekillendiği ve sınırlı akademik ilgi gördüğü bir başlangıç evresidir.

2010 sonrası dönemde yayın sayılarında kademeli bir artış başlamış, 2020 yılı itibarıyla bu artış belirgin hale gelmiştir. Dijital dönüşüm süreçlerinin hızlanması ve yapay zekânın bilgi hizmetlerine entegrasyonunun ivme kazanması, bu yükselişte etkili olmuştur. Özellikle 2023 yılında yayın sayısı zirveye ulaşarak alana yönelik akademik üretimin en yoğun olduğu yıl olmuştur.

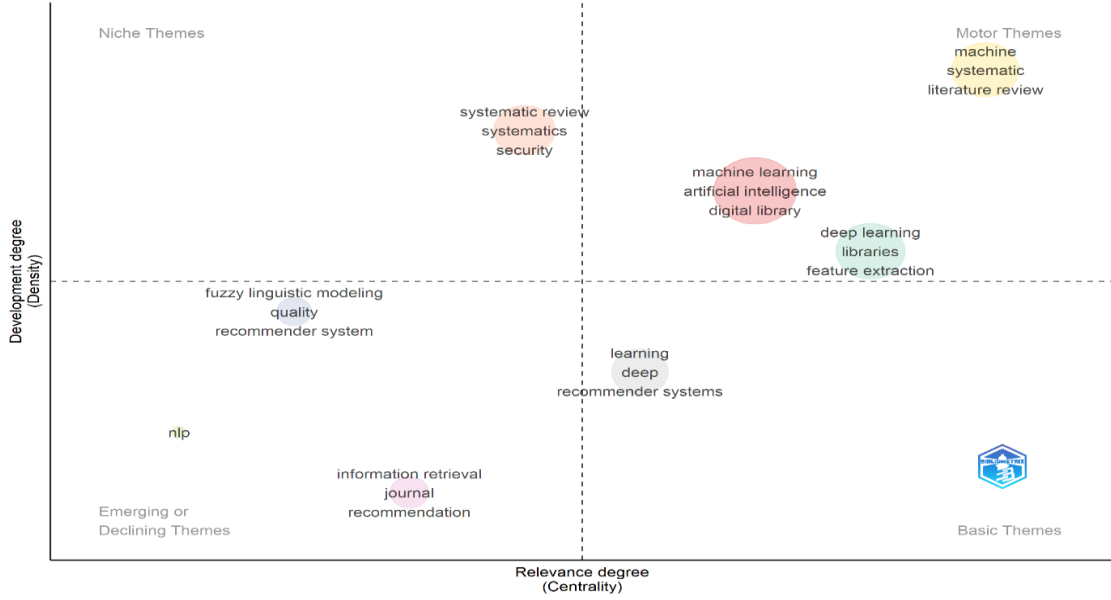
2025 yılına ait verilerde yayın sayısında düşüş gözlemlense de bu durumun yılın henüz tamamlanmamış olmasından kaynaklandığı düşünülmektedir. Genel olarak grafik, yapay zekâ ve dijital kütüphane kesişiminin bilimsel literatürde giderek daha fazla yer bulduğunu ve araştırma alanı olarak olgunlaşma sürecine girdiğini göstermektedir (Şekil 1).



Şekil 1. Yayınların yıllara göre dağılım grafiği.



Şekil 2. Anahtar kelime bulutu.



Şekil 3. Yazarın anahtar sözcüklerinin tematik haritası.

4.3. Anahtar Kelime Bulutu

Literatürde en sık kullanılan terimlerin görselleştirildiği anahtar kelime bulutu analizi, araştırma alanının tematik önceliklerini ve odaklandığı başlıca kavramları ortaya koymaktadır. Şekil 2’de yazarların anahtar sözcükleri (Author keywords) ile düzenlenen kelime bulutu görülmektedir. Kelimeler görülme sıklığı açısından, machine learning (33), artificial intelligence (26), deep learning (20), learning (11), digital library (10), systematic review (9), digital libraries (8) ve libraries (7) kavramları öne çıkmaktadır. Bu kavramlar, konuyla ilgili araştırma yaparken veya alana katkı sunacak yayın yaparken ortak bir zeminde buluşabilmek adına tercih edilmesi faydalı olabilecek kavramlara dair ipucu vermektedir.

Görselde dikkat çeken en büyük ve belirgin terimler arasında "machine learning" ve "artificial intelligence" yer almakta olup, bu durum çalışmalarda makine öğrenmesi ve yapay zekâ temelli yaklaşımların baskın olduğunu göstermektedir. Bu iki kavram, dijital kütüphanelerde bilgi işleme, kullanıcı davranışlarının modellenmesi ve veri tabanlı hizmet geliştirme gibi çok çeşitli alanlarda yoğun biçimde kullanıldığını işaret etmektedir.

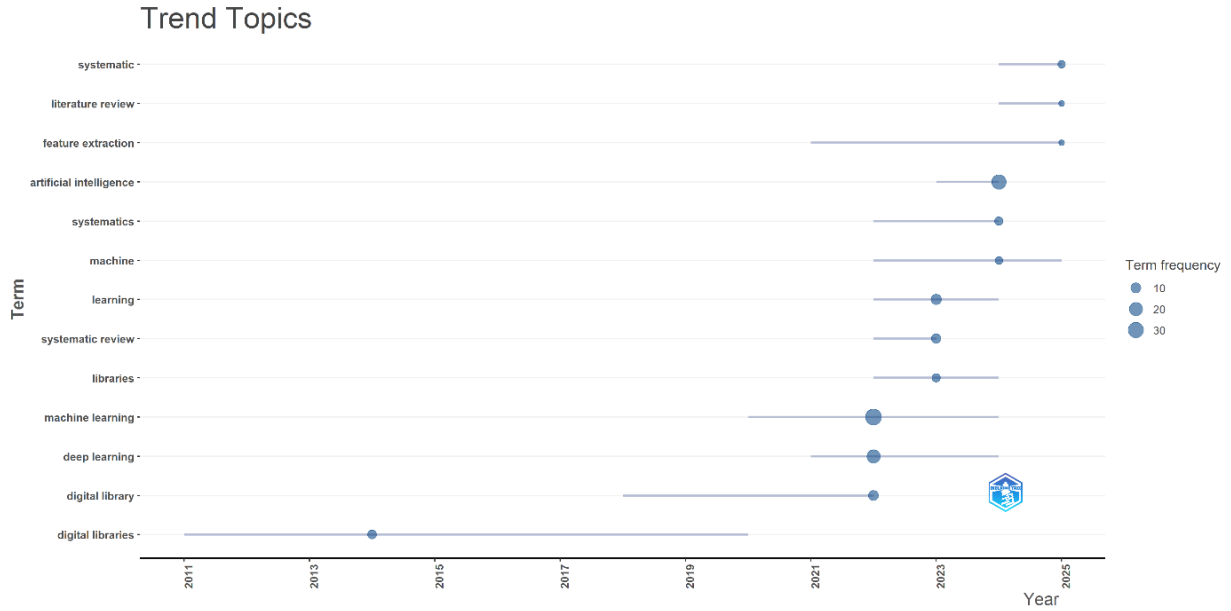
Öne çıkan diğer kavramlar arasında "deep learning", "digital library", "systematic review" ve "recommendation systems" gibi ifadeler yer almakta, bu

da literatürde derin öğrenme tabanlı tekniklerin yaygınlığını ve sistematik incelemelerin tercih edilen bir araştırma yöntemi olduğunu göstermektedir. Anahtar kelime bulutu, çalışmanın kavramsal çerçevesini görsel olarak destekleyerek, alanın entelektüel yapısını ve tematik yoğunlaşmalarını net biçimde yansıtmaktadır.

4.4. Anahtar Sözcüklerin Tematik Haritası

Tematik haritalar, bir araştırma alanındaki anahtar kavramların birlikte kullanılma sıklıklarına ve yapısal ilişkilerine göre gruplanarak, bilimsel alanın entelektüel yapısını görselleştiren analitik araçlardır. Şekil 3’de, anahtar sözcüklerle yapılan tematik harita görülmektedir. Bu harita, temaların gelişmişlik düzeyine (density) ve merkezilik derecesine (centrality) göre dört temel kategoriye ayrıldığını göstermektedir. Haritada yer alan her bir küme, anahtar kelimelerin birlikte görülme sıklıklarına göre oluşturulmuş ve araştırma alanındaki tematik yapıyı yansıtmaktadır.

Yazarın anahtar kelime tematik haritasına göre (Şekil 3), düğümlerdeki anahtar kelimeler yayınlarda kendi aralarında en yüksek oranda birlikte bulunma oranına sahip ağ kümeleridir. Buna göre, "learning, deep, recommender systems" en yüksek birlikte bulunma, merkezilik ve yoğunluğa sahip kümelerdir. Motor temalar bölümünde yer alan "machine learning, deep learning, machine" kümesi, alanda en çok çalışılan konulardır. Bu kavramlar, çalışmalarda hem teorik hem



Şekil 5. Trend kavramlar (trend topics).

Trend topics analizi ve anahtar kelime büyüklükleri birlikte değerlendirildiğinde, “systematic”, “literature review” ve “feature extraction” ile “machine learning”, “artificial intelligence” ve “deep learning” terimlerinin sık bir arada anıldığı sonucuna ulaşılmıştır (Şekil 5). Bu ilişki, sistematik inceleme yöntemlerinin makine öğrenimi ve derin öğrenme gibi ileri YZ tekniklerinin dijital kütüphanelerdeki uygulamalarını (örneğin, metin madenciliği, içerik analitiği) anlamak için yaygın bir şekilde kullanıldığını ortaya koymaktadır. “Feature extraction” teriminin öne çıkması, bu teknolojilerin veri işleme ve bilgi çıkarımı süreçlerinde kritik bir rol oynadığını, özellikle derin öğrenme ile entegre edildiğinde dijital kütüphane hizmetlerini geliştirmede etkili olduğunu göstermektedir.

Şekil 5’de vurgulanan trend topics, literatürün metodolojik ve teknolojik odaklarını yansıtmaktadır. “Machine learning”, “artificial intelligence” ve “deep learning” terimlerinin büyüklüğü, YZ’nin dijital kütüphanelerdeki dönüşümdeki merkezi rolünü doğrulamakta; “systematic” ve “literature review” terimlerinin varlığı ise alandaki araştırmaların sistematik ve kapsamlı bir yaklaşımla ele alındığını işaret etmektedir. Ancak, “feature extraction”ın trend topics arasında yer alması, literatürün henüz bu tekniğin dijital kütüphane bağlamındaki spesifik etkilerini tam anlamıyla araştırmadığını ve gelecekteki çalışmaların bu alana yönelmesi gerektiğini düşündürmektedir.

5. Tartışma

Bu çalışma, yapay zekâ ve dijital kütüphanelerin kesişimindeki literatürün bibliyometrik analizini gerçekleştirerek, alandaki entelektüel yapıyı ve araştırma eğilimlerini haritalandırmıştır. Anahtar kelime analizi, “machine learning” (241,6 defa), “deep learning” (171,5 defa) ve “artificial intelligence” (153,2 defa) terimlerinin yüksek birlikte görülme frekanslarıyla baskın olduğunu

ortaya koymuş, bu durum YZ’nin dijital kütüphanelerdeki yenilikçi uygulamalarda (örneğin, akıllı arama sistemleri, otomatik meta veri çıkarımı) merkezi bir rol oynadığını göstermektedir (Bornmann ve Mutz, 2015). Trend topics analizi ise “systematic”, “literature review” ve “feature extraction” kavramlarının öne çıktığını ve bu terimlerin “machine learning”, “artificial intelligence” ile “deep learning” ile sık bir arada anıldığını doğrulamıştır (Ellegaard ve Wallin, 2015). Bu bulgular, sistematik inceleme yöntemlerinin YZ tabanlı teknolojilerin dijital kütüphanelerdeki etkisini anlamada temel bir metodoloji sunduğunu ve özellik çıkarma tekniklerinin gelecekteki araştırmalar için potansiyel bir alan olduğunu ortaya koymaktadır.

Bulgular, literatürdeki yayın eğilimleriyle uyumludur; 1995–2005 yılları arasında sabit kalan yayın sayısı, 2005’ten itibaren artmış ve son beş yılda (2020–2025) önemli bir yükseliş göstermiştir. Bu artış, YZ teknolojilerinin dijital kütüphanelere entegrasyonunun akademik ilgiyle paralel olarak hız kazandığını ve özellikle makine öğrenimi ile derin öğrenme odaklı uygulamaların alandaki dönüşümde kilit bir rol oynadığını desteklemektedir (Vasishta vd., 2025). Ancak, “libraries” teriminin düşük frekansı (4,6 defa), dijital kütüphanelerin YZ ile entegrasyonunun henüz tam anlamıyla ayrı bir araştırma alanı olarak kristalleşmediğini ve literatürün daha geniş bir YZ bağlamına odaklandığını göstermektedir. Bu durum, Cox ve Mazumdar (2024)’ın YZ’nin kütüphane hizmetlerindeki tematik çeşitliliğe rağmen spesifik bir odak eksikliğine işaret eden görüşleriyle tutarlıdır.

Çalışmanın bir diğer önemli sonucu, etik ve toplumsal sorunların (örneğin, veri gizliliği, algoritmik önyargı) literatürde yeterince ele alınmamasıdır. “Feature extraction”ın trend topics arasında yer alması, YZ’nin veri işleme kapasitesinin önemini ortaya koysa da, bu teknolojilerin kullanıcı gizliliği ve hesap verebilirlik

üzerindeki etkileri hala sistematik bir şekilde incelenmemiştir (Johnson, 2017). Ayrıca, dijital eşitsizlik ve çoklu veri kaynaklarının karşılaştırmalı kullanımı gibi konuların eksikliği, alandaki araştırmaların bütüncül bir bakış açısına ihtiyaç duyduğunu göstermektedir (Hervieux ve Wheatley, 2021).

Sonuç olarak, bu çalışma, YZ'nin dijital kütüphanelerdeki dönüştürücü potansiyelini ve literatürdeki araştırma eğilimlerini aydınlatarak, makine öğrenimi ve derin öğrenme odaklı teknolojilerin alandaki merkezi rolünü teyit etmiştir. 06 Temmuz 2025 itibarıyla güncel verilere dayanan analiz, Şekil 4 ve Şekil 5'teki bulgularla desteklenerek, kütüphaneciler ve bilgi bilimciler için stratejik içgörüler sunmaktadır. Gelecekteki çalışmalar, etik sorunlara yönelik müdahaleleri, özellik çıkarma tekniklerini ve dijital kütüphane odaklı araştırmaları teşvik ederek, YZ destekli bilgi erişim sistemlerinin daha kapsayıcı ve adil bir şekilde geliştirilmesine katkı sağlayabilir.

6. Sonuç

Bu çalışma, yapay zekâ (YZ) ve dijital kütüphanelerin kesişimindeki literatürün bibliyometrik analizini gerçekleştirerek, bu alanda kapsamlı bir haritalandırma sunmuştur. 1995–2025 yılları arasında yayınlanan 195 makalenin analizi, son beş yılda (2020–2025) yayın sayısında artış olduğunu ve “machine learning” (241,6 defa), “deep learning” (171,5 defa) ile “artificial intelligence” (153,2 defa) terimlerinin baskın olduğunu göstermiştir. Trend topics analizi, “systematic”, “literature review” ve “feature extraction” kavramlarının öne çıktığını ve bu terimlerin YZ teknolojileriyle sık bir arada anıldığını ortaya koymuştur. Bu, sistematik incelemelerin ve özellik çıkarma tekniklerinin dijital kütüphanelerdeki yenilikleri anlamada kritik olduğunu teyit etmektedir.

Ancak, “libraries” teriminin düşük frekansı (4,6 defa) ve etik sorunların (örneğin, veri gizliliği, algoritmik önyargı) sınırlı ele alınması, alandaki araştırmaların dijital kütüphane bağlamına özgü derin bir odak geliştiremediğini göstermektedir. Vasishta vd. (2025) de belirttiği gibi, YZ'nin kütüphane uygulamalarındaki tematik çeşitlilik, etik boyutlara yeterince yönelmemektedir (Vasishta vd., 2025). Bu, YZ'nin potansiyelinin etik bir çerçeveye oturtulması gerektiğini vurgumaktadır.

Uluslararası işbirlikleri, YZ destekli dijital kütüphanelerin geliştirilmesinde umut vadetmektedir; ancak bu çabalar genellikle ulusal çapta kalmaktadır. Bu çalışma, etkili yazarları ve kurumları belirleyerek yeni araştırma hatlarını açığa çıkarmış ve “feature extraction”ın potansiyelini öne çıkarmıştır. 06 Temmuz 2025 itibarıyla güncel bulgular, Şekil 4 ve Şekil 5 ile desteklenerek, makine öğrenimi odaklı yeniliklerin alandaki rolünü teyit etmektedir.

Sonuç olarak, bu çalışma, YZ'nin dijital kütüphanelerdeki dönüştürücü etkisini belgeleyerek stratejik içgörüler sunmaktadır. Gelecekteki araştırmalar, etik müdahaleleri

ve uluslararası işbirliklerini teşvik ederek, daha adil ve etkili dijital kütüphane sistemleri geliştirmeye katkı sağlayabilir (Anand vd., 2012). Bu makale, sinerji yaratarak yeni projeleri teşvik etmeyi amaçlamaktadır (Cox ve Mazumdar, 2024).

Katkı Oranı Beyanı

Yazarın katkı yüzdeleri aşağıda verilmiştir. Yazar makaleyi incelemiş ve onaylamıştır.

%	E.D.
K	100
T	100
Y	100
VTI	100
VAY	100
KT	100
YZ	100
GR	100
PM	100

K= kavram, T= tasarım, Y= yönetim, VTI= veri toplama ve/veya işleme, VAY= veri analizi ve/veya yorumlama, KT= kaynak tarama, YZ= Yazım, GR= gönderim ve revizyon, PY= proje yönetimi.

Çatışma Beyanı

Yazar bu çalışmada hiçbir çıkar ilişkisi olmadığını beyan etmektedirler.

Etik Onay Beyanı

Bu araştırmada hayvanlar ve insanlar üzerinde herhangi bir çalışma yapılmadığı için etik kurul onayı alınmamıştır.

Kaynaklar

- Alam, M. J., Hassan, R., & Ogawa, K. (2023). Digitalization of higher education to achieve sustainability: Investigating students' attitudes toward digitalization in Bangladesh. *International Journal of Educational Research Open*, 5, 100273. <https://doi.org/10.1016/j.ijedro.2023.100273>
- Alemneh, D. G., Chang, H. C., Hawamdeh, S. M., Rorissa, A., & Assefa, S. (2019). Cybersecurity challenges in the era of open access and big data: Issues and considerations. *Proceedings of the Association for Information Science and Technology*, 56(1), 324-326. <https://doi.org/10.1002/pa2.32>
- Allison, D. (2012). Chatbots in the library: Is it time? *Library Hi Tech*, 30(1), 95-107. <https://doi.org/10.1108/07378831211213210>
- Anand, N., Yang, M., van Duin, J. R., & Tavasszy, L. (2012). GenCLOn: An ontology for city logistics. *Expert Systems with Applications*, 39(15), 11944-11960. <https://doi.org/10.1016/j.eswa.2012.03.068>
- Bornmann, L., & Mutz, R. (2015). Growth rates of modern science: A bibliometric analysis based on the number of publications and cited references. *Journal of the Association for Information Science and Technology*, 66(11), 2215-2222. <https://doi.org/10.1002/asi.23329>
- Campbell, D. G., & Cowan, S. R. (2016). The paradox of privacy: Revisiting a core library value in an age of big data and linked data. *Library Trends*, 64(3), 492-511. <https://doi.org/10.1353/lib.2016.0003>

- Cox, A. M., & Mazumdar, S. (2024). Defining artificial intelligence for librarians. *Journal of Librarianship and Information Science*, 56(2), 330-340. <https://doi.org/10.1177/09610006221142029>
- Deori, M., Kumar, V., & Verma, M. K. (2023). Analysis of YouTube video contents on Koha and DSpace, and sentiment analysis of viewers' comments. *Library Hi Tech*, 41(3), 711-728. <https://doi.org/10.1108/LHT-12-2020-0323>
- Ellegaard, O., & Wallin, J. A. (2015). The bibliometric analysis of scholarly production: How great is the impact? *Scientometrics*, 105(3), 1809-1831. <https://doi.org/10.1007/s11192-015-1645-z>
- Guleria, D., & Kaur, G. (2021). Bibliometric analysis of ecopreneurship using VOSviewer and RStudio Bibliometrix, 1989-2019. *Library Hi Tech*, 39(4), 1001-1024. <https://doi.org/10.1108/LHT-09-2020-0218>
- Hervieux, S., & Wheatley, A. (2021). Perceptions of artificial intelligence: A survey of academic librarians in Canada and the United States. *The Journal of Academic Librarianship*, 47(1), 102270. <https://doi.org/10.1016/j.acalib.2020.102270>
- Huo, Y. Q., Pan, X. H., Li, Q. B., Wang, X. Q., Jiao, X. J., Jia, Z. W., & Wang, S. J. (2015). Fifty top-cited classic papers in orthopedic elbow surgery: A bibliometric analysis. *International Journal of Surgery*, 18, 28-33. <https://doi.org/10.1016/j.ijso.2015.03.020>
- Islam, M. N., Aziz, M. T. B., & Chakravarty, R. (2022). Bibliometric analysis on information literacy (2017-2021): A systematic literature review. *Library Philosophy and Practice (e-journal)*, Article 7179. <https://digitalcommons.unl.edu/libphilprac/7179>
- Johnson, V. (2017). Leveraging technical library expertise for big data management. *Journal of the Australian Library and Information Association*, 66(3), 271-286. <https://doi.org/10.1080/24750158.2017.1356982>
- Kim, Y. S., & Cooke, L. (2017). Big data analysis of public library operations and services by using the Chernoff face method. *Journal of Documentation*, 73(3), 466-480. <https://doi.org/10.1108/JD-08-2016-0098>
- Martín-Del-Río, B., Solanes-Puchol, Á., Martínez-Zaragoza, F., & Benavides-Gil, G. (2018). Stress in nurses: The 100 top-cited papers published in nursing journals. *Journal of Advanced Nursing*, 74(7), 1488-1504. <https://doi.org/10.1111/jan.13566>
- Meng, Y., Chu, M. Y., & Chiu, D. K. (2023). The impact of COVID-19 on museums in the digital era: Practices and challenges in Hong Kong. *Library Hi Tech*, 41(1), 130-151. <https://doi.org/10.1108/LHT-03-2022-0127>
- Moed, H. F. (2009). New developments in the use of citation analysis in research evaluation. *Archivum Immunologiae et Therapiae Experimentalis*, 57(1), 13-18. <https://doi.org/10.1007/s00005-009-0001-5>
- Önder, O. K. (2025). Analysis of published manuscripts on Napoleon Bonaparte. *Black Sea Journal of Public and Social Sciences*, 8(1), 1-6. <https://doi.org/10.52704/bssocialscience.1541621>
- Tijjani, B., Ashiq, M., Siddique, N., Khan, M. A., & Rasul, A. (2021). A bibliometric analysis of quality research papers in Islamic finance: Evidence from Web of Science. *ISRA International Journal of Islamic Finance*, 13(1), 84-101. <https://doi.org/10.1108/IJIF-03-2020-0062>
- Tung, W. F., & Jara Santiago Campos, J. (2022). User experience research on social robot application. *Library Hi Tech*, 40(4), 914-928. <https://doi.org/10.1108/LHT-11-2020-0275>
- Vasishta, P., Dhingra, N., & Vasishta, S. (2025). Application of artificial intelligence in libraries: A bibliometric analysis and visualisation of research activities. *Library Hi Tech*, 43(2/3), 693-710. <https://doi.org/10.1108/LHT-06-2023-0245>
- Wijewickrema, M. (2023). A bibliometric study on library and information science and information systems literature during 2010-2019. *Library Hi Tech*, 41(2), 595-621. <https://doi.org/10.1108/LHT-06-2021-0210>
- Yu, P. Y., Lam, E. T. H., & Chiu, D. K. (2022). Operation management of academic libraries in Hong Kong under COVID-19. *Library Hi Tech*, 41(1), 108-129. <https://doi.org/10.1108/LHT-05-2021-0164>
- Zhang, K., & Lu, P. (2023). What are the key indicators for evaluating the service satisfaction of WeChat official accounts in Chinese academic libraries? *Library Hi Tech*, 41(3), 788-806. <https://doi.org/10.1108/LHT-01-2021-0008>



PHISHING ATAKLARININ BÜYÜK DİL MODELLERİ ÜZERİNE ETKİLERİ

Hakan Can ALTUNAY^{1*}

¹Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye

Özet: Büyük dil modellerinin (LLM) yaygın olarak uygulanması, önemli akademik ve toplumsal ilgiyi çeken yeni güvenlik zorluklarını ve etik endişeleri artırmıştır. LLM'lerin güvenlik açıklarının ve siber suçlarda kötüye kullanımının analizi, gelişmiş metin oluşturma yeteneklerinin kişisel gizlilik, veri güvenliği ve bilgi bütünlüğü için ciddi tehditler oluşturduğunu ortaya koymaktadır. Ayrıca, mevcut LLM tabanlı savunma stratejilerinin etkinliği incelenmiş ve değerlendirilmiştir. Bu çalışma, LLM'lerin phishing ataklarına karşı sosyal etkilerini incelemekte ve alanın gelişimini bilgilendirmeyi amaçlayan güvenlik uygulamaları ile etik yönetimlerini geliştirmek için gelecekteki uygulamaları önermektedir.

Anahtar kelimeler: LLM tabanlı tehdit azaltma, Kimlik avı atakları, Yapay zeka tabanlı kimlik avı

Effects of Phishing Attacks on Large Language Models

Abstract: The widespread application of large language models (LLMs) has raised new security challenges and ethical concerns that have attracted significant academic and societal attention. Analysis of LLMs' vulnerabilities and their misuse in cybercrime reveals that their advanced text generation capabilities pose serious threats to personal privacy, data security, and information integrity. Furthermore, the effectiveness of existing LLM-based defense strategies is examined and evaluated. This study examines the social implications of LLMs against phishing attacks and suggests future applications to enhance their security practices and ethical governance, aiming to inform the development of the field.

Keywords: LLM-based threat mitigation, Phishing attacks, AI-enabled phishing

*Sorumlu yazar (Corresponding author): Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye

E mail: hakancan.altunay@omu.edu.tr (H. C. ALTUNAY)

Hakan Can ALTUNAY  <https://orcid.org/0000-0002-0175-239X>

Gönderi: 08 Nisan 2025

Kabul: 01 Mayıs 2025

Yayınlanma: 15 Haziran 2025

Received: April 08, 2025

Accepted: May 01, 2025

Published: June 15, 2025

Cite as: Altunay, H. C. (2025). Effects of phishing attacks on large language models. *Black Sea Journal of Artificial Intelligence*, 1(1), 11–14.

1. Giriş

Son yıllarda, büyük dil modelleri (LLM'ler) doğal dil işlemede önemli ölçüde ilerleme kaydetti. Önemli örnekler arasında üretken önceden eğitilmiş dönüştürücü (GPT), BERT (Dönüştürücülerden Çift Yönlü Kodlayıcı Gösterimleri) ve T5 (Metinden Metne Aktarım Dönüştürücüsü) yer almaktadır (Annepaka ve Pakray, 2025). Bu modeller, metin oluşturma, makine çevirisi ve soru-cevap sistemleri gibi bir dizi görevde etkileyici performans göstermektedir. Ancak, bunların artan yaygınlığı güvenlik ve etik endişeleri artırarak hem akademiden hem de endüstriden dikkat çekmektedir (Zheng vd., 2025).

LLM'lerin ve üretken yapay zekanın yükselişi birçok endüstriyi derinden etkilemiştir. Eğitim, sağlık ve siyaset gibi sektörlerde, LLM'ler geleneksel iş süreçlerini dönüştürmektedir. Dijital dönüşümü ve akıllı gelişmeyi yönlendirirken verimliliği artırıyor ve maliyetleri düşürmektedirler. Ancak, bu hızlı ilerleme zorluklarla birlikte gelmektedir. Bilgi güvenliği ile ilgili olarak bakıldığında, LLM'ler yanlış bilgi üretebilir (Altunay,

2024a). Dikkat çekici bir örnek, CNET'in LLM tarafından oluşturulan makaleleri açık bir açıklama yapmadan yayınlamasıydı ve bu da potansiyel yanlış bilgiye ve şeffaflık eksikliğine yol açtı. Dahası, LLM'ler siber saldırılar için kötüye kullanılabilir. Bu karmaşık düşmanca saldırılar, zararlı içerikler üreterek yapay zeka güvenlik mekanizmalarından kaçınabilir. Bu, kimlik hırsızlığı ve toplumsal düzeni ve kişisel gizliliği tehdit eden kötü niyetli sosyal medya gönderileri de dahil olmak üzere önemli riskler oluşturur (Das vd., 2025). Dahası, LLM karar alma sürecindeki olası önyargılar ve adaletsizlik kapsamlı sosyo-etik tartışmaları ateşlemiştir. Eğitim verilerindeki önyargılar adaletsiz sonuçlara yol açabilir ve klişeleri güçlendirebilir. Ayrıca LLM'lerin Windows 11 seri numaraları gibi hassas bilgileri ifşa etmeye nasıl yönlendirilebileceğini göstermiştir. Bu sorunlar teknolojinin istikrarlı gelişimini engeller ve toplumsal uyum ve istikrara meydan okur (Zhu vd., 2025).

Bu çalışma, 2020'den Nisan 2025'e kadar bilgi güvenliği çerçevesinde LLM'lere gerçekleştirilen phishing



ataklarının kapsamlı bir genel görünümünü ve karşılaştırmasını sunmaktadır. Bu alandaki en son eğilimleri ve zorlukları açıklığa kavuşturmayı amaçlamaktadır. İlgili literatürü sentezleyerek ve analiz ederek, son yıllarda bu alanda bilgi güvenliği ve sosyal etikle ilişkili gizli riskler ortaya çıkarılmıştır. Tespit ve savunma teknikleri kategorize edilerek, hem kamu hem de profesyonel kuruluşlar için büyük dil modellerin bilgi ve etik güvenliği ve savunma mekanizmaları hakkında daha net bir anlayış sağlanmıştır. Bu çalışma, LLM'lerin güvenlik etiğine derinlemesine bir bakış sunarak, bilgi güvenliğine yönelik tehditlerin yanı sıra sosyal etik bağlamında savunma ve tespit tekniklerini vurgulamaktadır. Etik güvenliğin hayati bir parçası olarak bilgi güvenliği, teknolojinin güvenli ve sorumlu bir şekilde kullanılması için hayati öneme sahiptir. Birincil amacı, bilgileri ve sistemleri yetkisiz erişim, kullanım, hasar, müdahale veya yıkımdan korumaktır. Makalede, LLM'lerin karşılaşılabileceği olası sorunlar, işlevlerinin kötüye kullanılması ve kötü niyetli saldırılarla ilişkili riskler de dahil olmak üzere ele alınmaktadır. Bu tehditlere yanıt olarak, savunma ve tespit teknikleri ana hatlarıyla belirtilmiş ve model dağıtımından önce uygulanan stratejiler ve dağıtımdan sonra uygulanan acil durum önlemleri olarak kategorize edilmiştir.

2. Büyük Dil Modelleri ve Phishing Atakları

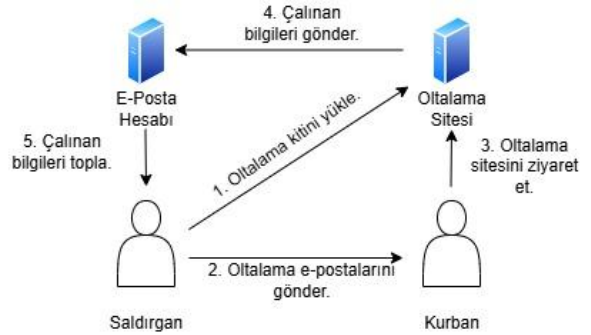
Günümüz dijital çağında, LLM'ler yapay zekada önemli bir teknolojidir. Hayatımızın birçok alanında yaygınlaşmıştır (Geren vd., 2025). Ancak, kullanımları genişledikçe bilgi güvenliği sorunları giderek daha önemli hale gelmektedir. Bu bölüm, LLM'lerin oluşturduğu başlıca güvenlik tehditlerini inceleyerek iki temel alana odaklanmaktadır: birincisi, LLM işlevlerinin kötüye kullanılmasından kaynaklanan güvenlik sorunları; ikincisi, LLM'lere yönelik kötü niyetli saldırılardan kaynaklanan endişeler.

Phishing ataklarının sayısı ChatGPT'nin kullanılmaya başlanması ile artmıştır. Çok yüksek meblağlarda zararlar veren phishing saldırılarından korunmak için kurum ve kuruluşlar personellerini eğitmeli ve doğru siber güvenlik araçları kullanmalıdır (Khonji vd., 2013). Polimorfik kimlik avı, bir e-postanın bileşenlerini rastgele hale getirerek aynı saldırının birçok farklı versiyonunu oluşturan gelişmiş bir kimlik avı biçimidir. Amaç, kara listelere veya imza tabanlı tespiti dayanan e-posta filtrelerini atlatmaktır. Bir e-postanın bir ögesi kötü amaçlı olarak tespit edilirse, bu öge saldırının diğer sürümlerinde farklı olacak ve tanınmayacaktır (Hadnagy, 2010).

Gelişmiş tespit araçları olmadan, polimorfik saldırılara karşı savunma yapmak zordur. Saldırının bir sürümü tespit edilse bile, varyasyonları çalışanların gelen kutularına ulaşabilir. Bu saldırılar, suç-hizmet-olarak-satılan kimlik avı kitlerinde bulunan otomasyon yöntemleri sayesinde giderek yaygınlaşmaktadır (Alabdan, 2020). Özetle, polimorfik saldırıların oluşturulması kolaydır ve imza tabanlı tespit

yazılımlarının tespit etmesi zordur (Bossetta, 2018).

Kimlik avı saldırıları, kullanıcı adları, parolalar ve kredi kartı bilgileri gibi hassas kullanıcı bilgilerini aldatma yoluyla elde etmeyi amaçlayan yaygın bir siber suç taktiğidir (Altunay, 2024b). Phishing ataklarının genel yapısı Şekil 1'de gösterilmiştir. Bu saldırılar iki türe ayrılabilir: büyük ölçekli kimlik avı ve hedefli kimlik avı (Xiao vd., 2025). Yapay zekadaki son gelişmeler, özellikle LLM'lerde, saldırganların son derece kişiselleştirilmiş ve ikna edici web tabanlı e-postalar oluşturmalarını sağlamıştır. Bu e-postalar genellikle geleneksel, kişiselleştirilmemiş e-postaların sınırlamalarını aşar (Altunay ve Albayrak, 2024). Ek olarak, LLM'lerin kültürler arası yetenekleri, saldırganların çabalarını belirli bölgelere veya dil gruplarına göre uyarlamalarına olanak tanır ve böylece aldatıcı taktiklerini güçlendirir (Wang vd., 2025). LLM tarafından oluşturulan metinler, güvenilir kuruluşların iletişim stillerini taklit ederek kullanıcı güvenliğini artırır (Quinn ve Thompson, 2024). Bu yetenek, spam filtrelerini ve güvenlik sistemlerini atlatmaya yardımcı olarak kimlik avı saldırılarının başarı oranlarını önemli ölçüde artırır (Kulkarni vd., 2025). Sonuç olarak, bu saldırıların ölçeğini ve otomasyonunu genişletir. Dahası, LLM'ler kimlik avı web sitelerinin oluşturulmasını ve başlatılmasını kolaylaştırarak saldırganların kapsamlı teknik becerilere ihtiyaç duymadan etkili dolandırıcılıklar gerçekleştirmesine olanak tanır. LLM'lerin yinelemeli öğrenme yetenekleri, saldırı stratejilerinin sürekli iyileştirilmesini sağlar, kimlik avı saldırılarını daha yaygın hale getirir ve ağ güvenliği için önemli tehditler oluşturur (Afane vd., 2024). Phishing saldırılarının genel yapısı Şekil 1'de verilmiştir.



Şekil 1. Phishing saldırılarının genel yapısı.

Hızlı Enjeksiyon Güvenlik Açığı, kullanıcı istemlerinin LLM'nin davranışını veya çıktısını istenmeyen şekillerde değiştirmesi durumunda ortaya çıkar. Bu girdiler, insanlar tarafından algılanamasa bile modeli etkileyebilir; bu nedenle, içerik model tarafından ayrıştırıldığı sürece, hızlı enjeksiyonların insanlar tarafından görülebilir/okunabilir olması gerekmez (Salt, 2009).

Hızlı Enjeksiyon güvenlik açıkları, modellerin istemleri nasıl işlediğinde ve girdilerin modeli, istem verilerini modelin diğer bölümlerine hatalı bir şekilde iletmeye

nasıl zorlayabileceğinde mevcuttur. Bu da, modelin kuralları ihlal etmesine, zararlı içerik oluşturmaya, yetkisiz erişime olanak sağlamasına veya kritik kararları etkilemesine neden olabilir. Geri Alma Artırılmış Üretimi (RAG) ve ince ayar gibi teknikler, LLM çıktıları daha alakalı ve doğru hale getirmeyi amaçlasa da, araştırmalar bunların hızlı enjeksiyon güvenlik açıklarını tamamen azaltmadığını göstermektedir (Boyd ve Keromytis, 2004). Hızlı enjeksiyon ve jailbreak, LLM güvenliğinde ilişkili kavramlar olsa da, genellikle birbirinin yerine kullanılırlar. Hızlı enjeksiyon, güvenlik önlemlerini atlatmayı da içerebilen davranışını değiştirmek için model yanıtlarını belirli girdiler aracılığıyla manipüle

etmeyi içerir. Jailbreak, saldırganın modelin güvenlik protokollerini tamamen göz ardı etmesine neden olan girdiler sağladığı bir tür hızlı enjeksiyondur. Geliştiriciler, hızlı enjeksiyon saldırılarını azaltmak için sistem komutlarına ve girdi işleme süreçlerine güvenlik önlemleri ekleyebilirler, ancak jailbreak'in etkili bir şekilde önlenmesi, modelin eğitim ve güvenlik mekanizmalarının sürekli güncellenmesini gerektirir (Zheng vd., 2024).

İnsanlar tarafından hazırlanan phishing saldırıları ile LLM'ler tarafından hazırlanan phishing saldırılarının etkilerinin karşılaştırılması Tablo 1'de gösterilmiştir.

Tablo 1. İnsan ve LLM kullanılarak hazırlanan phishing saldırılarının etkileri (Bethany vd., 2025)

E-Posta Yazarı	E-Posta Konusu	E-Posta Alıcıları	Açılan E-Posta Oranı	Tıklanan Bağlantı Oranı	Veri Girişi Oranı
İnsan	Kurum Amirinden Rapor	1541	%61,97	%21,67	%10,64
LLM	Kurum Amirinden Rapor	1490	%61,68	%21,34	%11,07
İnsan	Sürelili Oltalama	1591	%36,08	%6,66	%2,51
LLM	Sürelili Oltalama	1479	%40,37	%10,34	%4,19
İnsan	Genel Oltalama	1520	%54,67	%4,47	%1,18
LLM	Genel Oltalama	1508	%47,41	%4,84	%0,93

3. Tartışma ve Sonuç

LLM'ler çeşitli alanlarda giderek daha fazla kullanıldıkça, ilişkili bilgi güvenliği ve etik zorlukları daha belirgin hale geliyor. Bu makale, bilgi güvenliğindeki en son akademik gelişmelerden yararlanarak LLM'lerle ilgili güvenlik tehditlerini, savunma tekniklerini ve sosyo-etik sorunları analiz ediyor. Ayrıca, LLM'lerin oluşturduğu yeni güvenlik tehditlerini ortaya çıkarıyor. Bunlara kimlik avı saldırıları, kötü amaçlı yazılım tehditleri, bilgisayar korsanlığı olayları, sosyal mühendislik saldırıları, yanlış bilgilendirme ve LLM yeteneklerini istismar eden diğer kötüye kullanımlar dahildir. Ek olarak, model ters çevirme saldırıları, zehirleme saldırıları, arka kapı saldırıları, ipucu enjeksiyonları ve jailbreak saldırıları gibi riskler de bulunmaktadır. Makale ayrıca LLM güvenliğini artırmak için çeşitli stratejiler sunmaktadır. Teknolojinin sosyal etik üzerindeki etkisini ele alıyor ve otomatik düşmanca eğitim tekniklerinin geleceğini, çok dilli ortamlarda saldırı uyarlamalarının incelenmesini ve etik ve yasal çerçevelere olan ihtiyacı tartışıyor. Bu içgörüler, gelecekteki güvenlik uygulamaları ve LLM teknolojisinin gelişimi için güçlü bir teorik temel ve kapsamlı bir bakış açısı sağlar.

Katkı Oranı Beyanı

Yazarın katkı yüzdeleri aşağıda verilmiştir. Yazar makaleyi incelemiş ve onaylamıştır.

%	H.C.A.
K	100
T	100
Y	100
VTI	100
VAY	100
KT	100
YZ	100
GR	100
PM	100

K= kavram, T= tasarım, Y= yönetim, VTI= veri toplama ve/veya işleme, VAY= veri analizi ve/veya yorumlama, KT= kaynak tarama, YZ= Yazım, GR= gönderim ve revizyon, PY= proje yönetimi.

Çatışma Beyanı

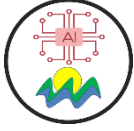
Yazar bu çalışmada hiçbir çıkar ilişkisi olmadığını beyan etmektedirler.

Etik Onay Beyanı

Bu çalışmada hayvanlar ve insanlar üzerinde herhangi bir çalışma yapılmadığı için etik kurul onayı alınmamıştır.

Kaynaklar

- Afane, K., Wei, W., Mao, Y., Farooq, J., & Chen, J. (2024). Next-generation phishing: How LLM agents empower cyber attackers. In *2024 IEEE International Conference on Big Data (Big Data)* (pp. 2558–2567). IEEE. <https://doi.org/10.1109/BigData62323.2024.10825316>
- Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, 12(10), 168. <https://doi.org/10.3390/fi12100168>
- Altunay, H. C. (2024a). Detection of SQL Injection attacks using machine learning algorithms based on NLP-based feature extraction. In *9th International Conference on Computer Science and Engineering (UBMK)* (pp. 468–472). IEEE. <https://doi.org/10.1109/UBMK62933.2024.10756715>
- Altunay, H. C. (2024b). Analysis of cyber attacks using honeypot. *Black Sea Journal of Engineering and Science*, 7(5), 954–959. <https://doi.org/10.52704/bssscience.1481075>
- Altunay, H. C., & Albayrak, Z. (2024). SMS spam detection system based on deep learning architectures for Turkish and English messages. *Applied Sciences*, 14(24), 11804. <https://doi.org/10.3390/app142411804>
- Annepaka, Y., & Pakray, P. (2025). Large language models: A survey of their development, capabilities, and applications. *Knowledge and Information Systems*, 67(3), 2967–3022. <https://doi.org/10.1007/s10115-024-02264-0>
- Bethany, M., Galiopoulos, A., Bethany, E., Karkevandi, M. B., Beebe, N., Vishwamitra, N., & Najafirad, P. (2025). Lateral phishing with large language models: A large organization comparative study. *IEEE Access*, 13, 60684–60701. <https://doi.org/10.1109/ACCESS.2025.3526685>
- Bossetta, M. (2018). The weaponization of social media: Spear phishing and cyberattacks on democracy. *Journal of International Affairs*, 71(2), 97–106.
- Boyd, S. W., & Keromytis, A. D. (2004). SQLrand: Preventing SQL injection attacks. In *Applied Cryptography and Network Security (ACNS 2004)* (pp. 292–302). Springer. https://doi.org/10.1007/978-3-540-24852-1_23
- Das, B. C., Amini, M. H., & Wu, Y. (2025). Security and privacy challenges of large language models: A survey. *ACM Computing Surveys*, 57(6), 1–39. <https://doi.org/10.1145/3690650>
- Geren, C., Board, A., Dagher, G. G., Andersen, T., & Zhuang, J. (2025). Blockchain for large language model security and safety: A holistic survey. *ACM SIGKDD Explorations Newsletter*, 26(2), 1–20. <https://doi.org/10.1145/3706497.3706500>
- Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.
- Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091–2121. <https://doi.org/10.1109/SURV.2013.032213.00001>
- Kulkarni, A., Balachandran, V., Divakaran, D. M., & Das, T. (2024). From ML to LLM: Evaluating the robustness of phishing webpage detection models against adversarial attacks. *Digital Threats: Research and Practice*, 6(2), 1–25. <https://doi.org/10.1145/3696455>
- Quinn, T., & Thompson, O. (2024). *Applying large language model (LLM) for developing cybersecurity policies to counteract spear phishing attacks on senior corporate managers* [Preprint]. Research Square. <https://doi.org/10.21203/rs.3.rs-4405206/v1>
- Salt, C. (2009). *SQL injection attacks and defense*. Elsevier (Syngress).
- Wang, S., Zhao, Y., Hou, X., & Wang, H. (2025). Large language model supply chain: A research agenda. *ACM Transactions on Software Engineering and Methodology*, 34(5), 1–46. <https://doi.org/10.1145/3702995>
- Xiao, X., Zhang, Y., Xu, J., Ren, W., & Zhang, J. (2025). Assessment methods and protection strategies for data leakage risks in large language models. *Journal of Industrial Engineering and Applied Science*, 3(2), 6–15.
- Zheng, J., Qiu, S., Shi, C., & Ma, Q. (2025). Towards lifelong learning of large language models: A survey. *ACM Computing Surveys*, 57(8), 1–35. <https://doi.org/10.1145/3703155>
- Zheng, X., Pang, T., Du, C., Liu, Q., Jiang, J., & Lin, M. (2024). Improved few-shot jailbreaking can circumvent aligned language models and their defenses. *Advances in Neural Information Processing Systems (NeurIPS)*, 37, 32856–32887.
- Zhu, X., Zhou, W., Han, Q. L., Ma, W., Wen, S., & Xiang, Y. (2025). When software security meets large language models: A survey. *IEEE/CAA Journal of Automatica Sinica*, 12(2), 317–334. <https://doi.org/10.1109/JAS.2024.410762>



JAVASCRIPT FONKSİYONLARINDA GÜVENLİK AÇIKLARININ MAKİNE ÖĞRENMESİ YÖNTEMLERİYLE TESPİTİ

Hasan Hüseyin ALAV^{1*}, Özgür TONKAL¹, Zafer CÖMERT¹

¹Samsun University, Faculty of Engineering and Natural Sciences, Department of Software Engineering, 55080, Samsun, Türkiye

Özet: JavaScript, modern web uygulamalarında temel bir programlama dili haline gelmiştir. Ancak dinamik ve zayıf tür denetimine sahip yapısı, ciddi güvenlik açıklarının ortaya çıkmasına neden olmaktadır. Bu çalışmada, JavaScript kod parçacıklarındaki güvenlik açıklarını otomatik olarak tespit etmek amacıyla geliştirilen makine öğrenmesi tabanlı yeni bir çerçeve olan JSVULNDETECT önerilmektedir. Geleneksel manuel kod inceleme yöntemlerinin hata yapmaya eğilimli ve zaman açısından verimsiz olması, otomatik ve ölçeklenebilir analiz araçlarına olan ihtiyacı artırmaktadır. Çalışma kapsamında, özenle ön işlenmiş ve denge sağlanmış bir veri kümesi üzerinde Random Forest, XGBoost, LightGBM ve Destek Vektör Makineleri (SVM) gibi toplamda on iki farklı makine öğrenmesi algoritması değerlendirilmiştir. Veri kümesindeki sınıf dengesizliği SMOTE-Tomek yöntemiyle giderilmiş; modellerin performansı ise Bayesyen hiperparametre optimizasyonu ile artırılmıştır. Ayrıca, Topluluk Öğrenmesi (Ensemble Learning) yaklaşımları olan Oylama (Voting) ve Yığınlama (Stacking) stratejileri uygulanmış, en yüksek doğruluk oranı %97,51 ile Stacking Sınıflandırıcısı kullanılarak elde edilmiştir. Önerilen çerçeve, çoklu öğrenme yaklaşımlarını birleştirerek güvenlik açığı tespit performansını artırmakta ve gerçek zamanlı analiz için web tabanlı bir arayüz sunmaktadır. Bu yönüyle çalışma, mevcut literatürde raporlanan sonuçları aşmakta ve geliştiriciler ile güvenlik analistleri için pratik bir analiz aracı olarak değerli bir katkı sunmaktadır.

Anahtar kelimeler: Siber güvenlik, Makine öğrenmesi, Javascript güvenliği, Güvenlik açığı tespiti, Kod güvenliği

Detection of Security Vulnerabilities in Javascript Functions Using Machine Learning Methods

Abstract: JavaScript has become an essential programming language in modern web applications; however, its dynamic and loosely-typed nature introduces considerable security vulnerabilities. This paper presents JSVULNDETECT, a novel machine learning-based framework designed to automatically detect vulnerabilities in JavaScript code segments. Unlike traditional manual review approaches, which are often error-prone and inefficient, our system offers a scalable, automated solution for static code analysis. We evaluate and compare twelve machine learning algorithms—such as Random Forest, XGBoost, LightGBM, and Support Vector Machines—using a carefully preprocessed and balanced dataset. To address class imbalance, we apply the SMOTE-Tomek method, and we optimize model performance via Bayesian hyperparameter search. Moreover, we integrate ensemble learning strategies (Voting and Stacking), achieving a maximum accuracy of 97.51% with the Stacking Classifier. Our work advances the field by combining multiple learning paradigms, enhancing detection performance, and providing a web-based interface for real-time analysis. The proposed framework not only surpasses previous results reported in similar studies but also serves as a practical tool for developers and security analysts in identifying potential threats in JavaScript functions.

Keywords: Cybersecurity, Machine learning, Javascript security, Vulnerability detection, Code security

*Sorumlu yazar (Corresponding author): Samsun University, Faculty of Engineering and Natural Sciences, Department of Software Engineering, 55080, Samsun, Türkiye

E mail: hhsynalv@gmail.com (H. H. ALAV)

Hasan Hüseyin ALAV  <https://orcid.org/0009-0001-1812-2706>

Özgür TONKAL  <https://orcid.org/0000-0001-7219-9053>

Zafer CÖMERT  <https://orcid.org/0000-0001-5256-7648>

Gönderi: 14 Nisan 2025

Kabul: 01 Mayıs 2025

Yayınlanma: 15 Haziran 2025

Received: April 14, 2025

Accepted: May 01, 2025

Published: June 15, 2025

Cite as: Alav, H. H., Tonkal, Ö., & Cömert, Z. (2025). Detection of security vulnerabilities in Javascript functions using machine learning methods. *Black Sea Journal of Artificial Intelligence*, 1(1), 15–24.

1. Giriş

Web tabanlı uygulamaların hızla yaygınlaşmasıyla birlikte, JavaScript programlama dili hem istemci tarafında (client-side) hem de sunucu tarafında (server-side) en çok kullanılan teknolojilerden biri haline gelmiştir. Özellikle Node.js'in yaygınlaşmasıyla birlikte, JavaScript yalnızca dinamik web sayfalarının değil, aynı zamanda sunucu tarafı servislerin de temel yapı taşı olmuştur (Ferenc vd., 2019). Bu yaygın kullanım, beraberinde ciddi güvenlik sorunlarını da gündeme getirmiştir. JavaScript'in dinamik ve zayıf biçimlendirilmiş yapısı, geliştiricilere büyük esneklik

sağlarken; aynı zamanda kod enjeksiyonu, siteler arası betik çalıştırma [Cross-Site Scripting (XSS)] ve siteler arası istek sahteciliği [Cross-Site Request Forgery (CSRF)] gibi birçok saldırı türü için de uygun bir zemin hazırlamaktadır (Breiman, 2001; Friedman, 2001). Geleneksel güvenlik analiz yöntemleri genellikle manuel kod incelemelerine veya klasik statik analiz araçlarına dayanmaktadır. Ancak bu yöntemler hem zaman alıcıdır hem de insan hatasına açık olması nedeniyle yüksek güvenilirlik sağlayamamaktadır (Geurts vd., 2006). Son yıllarda, yapay zekâ ve özellikle makine öğrenmesi tabanlı yaklaşımlar, güvenlik zafiyetlerinin otomatik



tespiti konusunda umut vaat eden çözümler sunmaya başlamıştır. Bu yöntemler, yazılım kodlarını istatistiksel olarak inceleyerek olası açıklara dair tahminlerde bulunabilmekte ve sürekli güncellenebilir modeller sayesinde uyarlanabilir (adaptif) güvenlik analizleri gerçekleştirebilmektedir (Hosmer ve Lemeshow, 2000). Literatürde bu alanda yapılan çalışmalarda, farklı makine öğrenmesi tekniklerinin JavaScript, C/C++ ve Python gibi programlama dillerindeki güvenlik açıklarının sınıflandırılması amacıyla kullanıldığı görülmektedir. Örneğin, Ferenc vd. (2019) JavaScript fonksiyonları üzerinde çeşitli makine öğrenmesi algoritmalarını karşılaştırarak güvenlik açığı tespiti gerçekleştirmiştir. Benzer şekilde, Chen ve Guestrin (2016) tarafından geliştirilen XGBoost algoritması, yüksek performanslı ağaç tabanlı öğrenme yöntemleriyle birçok sınıflandırma probleminde başarı göstermiştir. Ancak bu çalışmaların çoğu, sınırlı sayıda model ve parametrik yapı ile çalıştığından, sistemin genellenebilirliğini ve doğruluk oranlarını sınırlamaktadır.

Bu çalışmanın amacı, JavaScript fonksiyonları içerisindeki potansiyel güvenlik açıklarını otomatik olarak tespit edebilen, yüksek doğruluk ve genellenebilirliğe sahip bir makine öğrenmesi sistemi geliştirmektir. Özgün katkı olarak:

- 12 farklı sınıflandırma modeli sistematik biçimde karşılaştırılmış,
- SMOTE-Tomek ile veri dengesizliği giderilmiş,
- Hyperopt algoritmasıyla hiperparametre optimizasyonu yapılmış,
- Sonuçların kararlılığı Voting ve Stacking gibi topluluk (ensemble) yöntemleri ile güçlendirilmiştir.

Bu yapı sayesinde, doğruluk oranı %97,51 seviyesine ulaşmış ve literatürdeki benzer çalışmalardan daha yüksek performans elde edilmiştir. Ayrıca geliştirilen JSVULNDETECT sistemi, kullanıcı dostu bir web arayüzü ile JavaScript kodlarını otomatik analiz edebilmekte; böylece hem akademik hem de endüstriyel ortamlarda kullanılabilecek bir güvenlik değerlendirme aracı sunmaktadır.

2. Literatür Özeti

Bu bölümde, JavaScript tabanlı yazılımlarda güvenlik açığı tespitine yönelik çalışmalar kapsamlı bir şekilde incelenmiş, makine öğrenmesi yöntemlerinin bu alandaki kullanımı değerlendirilmiştir. İlk olarak, güvenlik açığı tespiti üzerine gerçekleştirilen önceki çalışmalar ele alınarak mevcut yöntemlerin güçlü ve zayıf yönleri tartışılmıştır. Ardından, JavaScript programlama dili özelinde geliştirilen makine öğrenmesi uygulamaları incelenmiş ve bu yaklaşımların siber güvenlik bağlamındaki katkıları ortaya konmuştur. Son olarak, bu çalışmanın literatürdeki yeri belirlenerek mevcut boşluklar ve araştırmanın özgün yönleri vurgulanmıştır. Bu bölüm, önerilen sistemin alana nasıl bir katkı sunduğunu teorik temeller üzerinden açıklamayı

amaçlamaktadır.

2.1. Güvenlik Açığı Tespiti Üzerine Yapılan Çalışmalar

Yazılım güvenliği, özellikle web uygulamalarının yaygınlaşmasıyla birlikte hem akademik dünyada hem de endüstride büyük ilgi gören bir araştırma alanı haline gelmiştir. Geleneksel güvenlik testleri genellikle manuel kod incelemesine veya temel statik analiz araçlarına dayanmakta; ancak bu yöntemler, yüksek hata oranı ve düşük ölçeklenebilirlik gibi sınırlamalar nedeniyle günümüz yazılım sistemlerinin ihtiyaçlarını karşılamada yetersiz kalmaktadır (Hosmer ve Lemeshow, 2000). Bu nedenle, güvenlik açıklarının otomatik olarak tespit edilmesine yönelik yapay zekâ ve makine öğrenmesi tabanlı yaklaşımlar son yıllarda öne çıkmıştır.

Gradient Boosting yöntemi, kod örüntülerindeki karmaşık ilişkileri modellemede başarılı sonuçlar elde etmiş ve güvenlik açığı tespitinde sıkça başvurulan modellerden biri olmuştur (Friedman, 2001). Benzer şekilde, Random Forest algoritması yüksek varyansa sahip verilerde dengeli sonuçlar vermesi ve aşırı öğrenmeye (overfitting) karşı dayanıklı yapısı sayesinde yazılım güvenliği alanında tercih edilen algoritmalarından biri haline gelmiştir (Breiman, 2001).

XGBoost algoritması, büyük boyutlu ve dengesiz veri kümeleri üzerinde etkili performans sunarak yazılım güvenliği bağlamında öne çıkmıştır (Chen ve Guestrin, 2016). Bununla birlikte, Extremely Randomized Trees modeli, klasik karar ağaçlarının rastgeleleştirilmiş versiyonu ile daha esnek bir yapı sunarak güvenlik açığı tespiti gibi karmaşık problemler için alternatif bir çözüm getirmiştir (Geurts vd., 2006).

Ferenc vd. (2019), JavaScript fonksiyonları üzerinde gerçekleştirdikleri çalışmalarında, çeşitli makine öğrenmesi algoritmalarının güvenlik açığı tespitindeki başarılarını karşılaştırmalı olarak analiz etmişlerdir. Bu çalışmada, karar ağaçları, Destek Vektör Makineleri (SVM) ve Naive Bayes gibi yöntemlerin farklı doğruluk oranları sergilediği ve sınıflandırma başarısının model seçimi kadar veri ön işleme tekniklerine de bağlı olduğu sonucuna ulaşılmıştır.

Bu alanda yapılan çalışmalar, genel olarak sınırlı sayıda modelle ve sınırlı parametreler üzerinde yoğunlaşmıştır. Ayrıca, verinin dengesiz dağılımı, özellik mühendisliği (feature engineering) süreçlerinin belirsizliği ve kullanılan metriklerin çeşitliliği, sonuçların karşılaştırılabilirliğini zorlaştırmaktadır. Bu durum, daha kapsamlı, çoklu model tabanlı ve entegratif sistemlere olan ihtiyacı doğurmuştur.

2.2. JavaScript Üzerine Makine Öğrenmesi Uygulamaları

JavaScript'in hem istemci hem de sunucu tarafında yaygın biçimde kullanılması, bu dili hedef alan güvenlik açıklarının da daha sık karşılaşılmaya yol açmaktadır. JavaScript, özellikle Belge Nesne Modeli (Document Object Model [DOM]) manipülasyonu, kullanıcı girişleri ve üçüncü parti entegrasyonlar gibi işlemlerde yüksek risk taşıyan bir yapıya sahiptir. Bu nedenle, bu dile özgü

güvenlik açıklarının (örneğin, XSS, DOM tabanlı enjeksiyonlar ve güvensiz API kullanımları) tespit edilmesi için özel çalışmalar yapılmaktadır.

Ferenc vd. (2019), JavaScript fonksiyonları üzerinde gerçekleştirdikleri bir çalışmada, statik analiz araçlarıyla birlikte makine öğrenmesi yöntemlerini entegre ederek güvenlik açığı içeren fonksiyonların sınıflandırılmasını gerçekleştirmiştir. Bu çalışmada, farklı sınıflandırma algoritmalarının performansları karşılaştırılmış ve doğru özellik mühendisliğinin (feature engineering) başarıyı belirgin şekilde etkilediği vurgulanmıştır.

McCallum ve Nigam (1998) tarafından önerilen Naive Bayes modelinin metin tabanlı analizlerdeki başarısı, JavaScript kodları üzerindeki analizlerde de uygulanabilirliğini göstermiştir. JavaScript kodları doğrudan metin olarak değerlendirilebildiğinden, n-gram tabanlı özellik çıkartımı ile bu tür algoritmalar etkili şekilde kullanılabilir.

Son yıllarda, derin öğrenme modelleri de JavaScript güvenliği bağlamında araştırılmaya başlanmıştır. Örneğin, kodu Soyut Sözdizim Ağacı (Abstract Syntax Tree [AST]) yapısına dönüştürerek kodun yapısal özelliklerini öğrenmeye çalışan projeler, Evrişimsel Sinir Ağı (Convolutional Neural Network [CNN]) veya Tekrarlayan Sinir Ağı (Recurrent Neural Network [RNN]) tabanlı yaklaşımlar kullanarak zararlı davranış örüntülerini sınıflandırma hedefiyle geliştirilmektedir. Ancak bu tür modeller yüksek hesaplama gücü gerektirdiğinden, pratikte kullanımı sınırlı kalabilmektedir.

Son yıllarda yazılım güvenlik açıklarının tespitine yönelik makine öğrenmesi tabanlı yaklaşımlar önemli ilerlemeler kaydetmiştir. Harzevili vd. (2023), 2011–2022 yılları arasındaki 67 çalışmayı inceleyerek veri dengesizliği, özellik çıkarımı, model genellemesi ve açıklanabilirlik konularında süregelen sorunları vurgulamış ve yeni nesil yöntemlere yönelim ihtiyacını ortaya koymuştur. JavaScript özelinde geliştirilen modern yöntemler, geleneksel istatistiksel sınıflandırıcıların ötesine geçmektedir. Örneğin PeerJ Computer Science’ta yayımlanan 2024 tarihli bir çalışma, JavaScript fonksiyonlarındaki güvenlik zafiyetlerini tespit etmek amacıyla çok katmanlı konvolüsyonel sinir ağlarını istifleyerek (stacking-CNN) önemli ölçüde doğruluk artışı sağlamıştır. Benzer şekilde, Liu vd. (2023) tarafından sunulan MFXSS modeli, kaynak kodun soyut sözdizim ağaçları (AST) ve kontrol akış grafikleri (CFG) üzerinden çoklu özellik füzyonu gerçekleştirerek, özellikle XSS açıklarının tespitinde yüksek performans sergilemiştir. Bu güncel çalışmalar, yazılım güvenlik açığı tespitinde derin öğrenme ve grafik tabanlı modelleme tekniklerinin giderek daha fazla benimsendiğini ve geleneksel yöntemlere kıyasla daha üstün sonuçlar sunduğunu göstermekte olup, bu çalışmanın da benzer bir motivasyonu desteklediğini teyit etmektedir.

Güncel çalışmalar, genellikle tek bir modelin performansına odaklanmakta ve topluluk öğrenme (ensemble) yöntemlerinin potansiyelinden yeterince

yararlanmamaktadır. Ayrıca, hiperparametre optimizasyonu, veri ön işleme ve sınıf dengesizliği gibi konular çoğu zaman yüzeysel ele alınmakta; bu da sistemlerin genelleme kabiliyetini düşürmektedir.

Bu bağlamda, JavaScript kodlarının güvenlik analizi için optimize edilmiş, çoklu model karşılaştırmalı ve topluluk öğrenme yöntemlerinden faydalanan sistemlere olan ihtiyaç giderek artmaktadır. Bu çalışmanın önemli motivasyon kaynaklarından biri de bu eksikliği giderecek yapısal bir çözüm sunabilmektir.

Literatürdeki mevcut çalışmalar incelendiğinde, güvenlik açığı tespiti konusunda makine öğrenmesi tabanlı yaklaşımların giderek daha fazla tercih edildiği görülmektedir. Bununla birlikte, bu çalışmaların büyük çoğunluğu sınırlı sayıda model üzerinde yoğunlaşmakta; veri dengesizliği, hiperparametre optimizasyonu ve topluluk öğrenme (ensemble) yöntemlerinin birlikte uygulanması gibi önemli boyutlar genellikle göz ardı edilmektedir. Özellikle JavaScript özelinde yapılan çalışmalarda, sınıflandırma modelleri ile güvenlik açığı içeren kodların tespiti hedeflenmiş olsa da, bu sistemlerin çoğu tekil algoritmalarla geliştirilmiş ve geniş kapsamlı karşılaştırmalar yapılmamıştır.

Ayrıca, literatürdeki bazı çalışmalar sınıflandırma başarısını değerlendirmek için yalnızca doğruluk (accuracy) metriğini kullanmakta; bu da özellikle dengesiz veri kümelerinde yanıltıcı sonuçlara yol açabilmektedir. Topluluk öğrenme yöntemlerinin (özellikle çok katmanlı yığınlama [Stacking] gibi yaklaşımların) bu bağlamda sunduğu avantajlar yeterince araştırılmamış; kullanılan veri ön işleme tekniklerinin (örneğin, Sentetik Azınlık Aşırı Örnekleme Tekniği ve Tomek bağlantıları [SMOTE-Tomek] gibi hibrit dengeleme yöntemleri) sınıflandırma performansı üzerindeki etkisi ayrıntılı olarak değerlendirilmemiştir. Bu çalışma, literatürdeki bu boşlukları doldurmayı hedeflemektedir. Özgün yönleri şunlardır:

- 12 farklı makine öğrenmesi modeli detaylı şekilde karşılaştırılmıştır.
- Her bir model için Bayes optimizasyonu (Bayesian Optimization) tabanlı hiperparametre ayarı yapılmıştır.
- Veri kümesindeki sınıf dengesizliği SMOTE-Tomek yöntemi ile ele alınmıştır.
- Hem oy birliği temelli (Voting) hem de yığınlama temelli (Stacking) topluluk öğrenme yöntemleri kullanılarak, modellerin yatay ve dikey güçlü yönleri bir araya getirilmiştir.
- Elde edilen sistem, %97,51 doğruluk oranıyla önceki çalışmalardan daha iyi performans göstermiştir.
- Ayrıca, sistemin web arayüzü ile kullanılabilir hale getirilmiş olması, akademik prototipten çok endüstriyel geçerliliği olan bir yapıya işaret etmektedir.

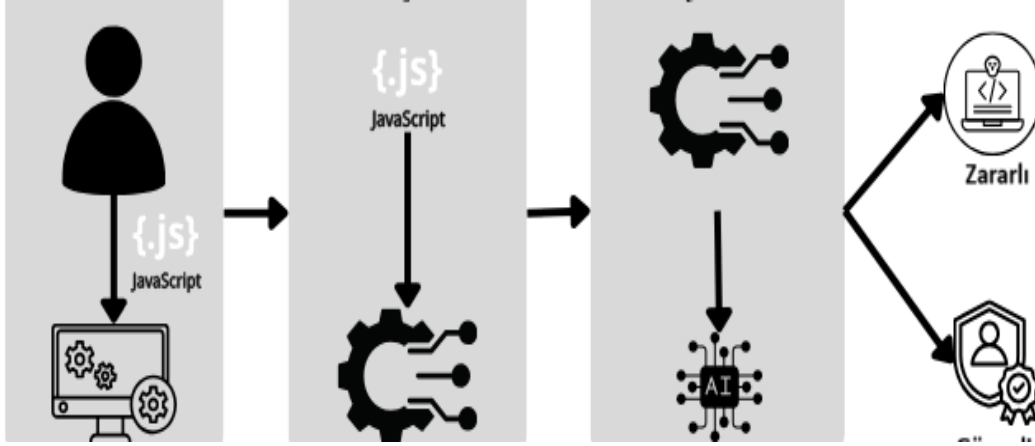
Bu yönleriyle çalışma hem yöntemsel bütünlüğü hem de uygulamaya dönük yapısıyla mevcut literatüre anlamlı bir katkı sunmaktadır.

3. Materyal ve Yöntem

Bu bölümde çalışmanın uygulama adımları, kullanılan veri seti, veri ön işleme süreci, özellik çıkarımı, veri dengeleme yöntemleri ve sınıflandırma modelleri ayrıntılı olarak sunulmaktadır. Genel sistem mimarisi Şekil 1’de gösterilmektedir.

Şekil 1’ de geliştirilen sistemin genel işleyiş süreci üç aşamalı olarak sunulmuştur. İlk aşamada, kullanıcı sisteme analiz edilmek üzere bir JavaScript kodu

yüklemektedir. Bu kod, ikinci aşamada sistem tarafından incelenerek makine öğrenmesi için gerekli olan temel özellikler (nitelikler) otomatik olarak çıkarılmaktadır. Son aşamada ise, bu özellikler kullanılarak kodun güvenlik açığı içerip içermediği analiz edilmekte ve kullanıcıya bilgi verilmektedir. Böylece geliştiriciler, yazdıkları kodlarda potansiyel güvenlik açıklarını hızlı ve etkili bir şekilde tespit etme imkânına sahip olmaktadır.



Şekil 1. Akış diyagramı.

3.1. Veri Seti

Bu çalışmada kullanılan veri seti, Ferenc ve arkadaşları tarafından geliştirilen ve JavaScript fonksiyonlarının güvenlik zafiyeti içerip içermediğini sınıflandırmayı amaçlayan etiketli bir veri kümesidir (Ferenc vd., 2019). Veri seti toplamda 10.000'den fazla JavaScript fonksiyonu içermekte olup, her bir fonksiyon için 45'ten fazla statik özellik (örneğin: kod uzunluğu, döngü karmaşıklığı, hata geçmişi, ifade sayısı vb.) hesaplanmıştır. Fonksiyonlar, güvenli (non-vulnerable) ve güvensiz (vulnerable) olmak üzere iki sınıfa ayrılmıştır. Ancak sınıflar arasında ciddi bir dengesizlik bulunmaktadır: veri setinde güvenli fonksiyonlar yaklaşık %85'lik bir çoğunlukla temsil edilirken, güvensiz fonksiyonlar yalnızca %15 oranındadır. Bu dengesizlik, modelin güvensiz fonksiyonları öğrenmesini zorlaştırmakta ve sınıflandırma başarımını düşürmektedir.

Bu nedenle, veri seti üzerinde Sentetik Azınlık Aşırı Örneklem Tekniği (SMOTE) ile Tomek bağlantılarının birleştirilmesinden oluşan SMOTE-Tomek yöntemi uygulanarak sınıf dengesi sağlanmış ve öğrenme algoritmalarının pozitif sınıf (güvensiz fonksiyon) performansı artırılmıştır. Veri seti, hem temel hem de türetilmiş özellikleri içermesi sayesinde, yalnızca makine öğrenmesi algoritmalarını test etmek için değil, aynı zamanda özellik mühendisliği (feature engineering) süreçlerini de değerlendirmek açısından zengin bir kaynak sunmaktadır.

3.2. Özellik Çıkarımları

Veri setinde bulunan özellikler, JavaScript fonksiyonlarının güvenlik açıklarını tespit etmek için

kritik öneme sahiptir. Bu çalışmada kullanılan bazı temel özellikler Tablo 1’de gösterilmiştir.

Tablo 1. Kullanılan özellikler

Özellik Kodu	Açıklama
LOC (Lines of Code)	Bir fonksiyonun toplam kod satırı sayısı
CYCL_DENS(Cyclomatic Density)	Fonksiyonun döngüsel karmaşıklık yoğunluğu
HBUGS (Historical Bugs)	Fonksiyonun geçmişte içerdiği hata sayısı
NOS(Number of Statements)	Fonksiyon içerisindeki toplam ifade sayısı
HDIFF(Historical Diff)	Fonksiyonun geçmişte yapılan değişikliklerin sayısı

Bu özellikler, güvenlik açıklarını tespit etmek için kullanılan temel metriklerdir. Ayrıca, bu çalışmada bu temel özelliklerden türetilen yeni özellikler de Tablo 2’de gösterilmiştir.

Bu özellik çıkarımları, veri setinin zenginleştirilmesi ve daha hassas analizler yapılması için kritik öneme sahiptir.

3.3. Veri Dengesizliğinin Giderilmesi

Veri dengesizliği problemi, güvenlik açığı bulunmayan örneklerin veri setinde baskın olması nedeniyle ortaya çıkmaktadır. Bu sorunu çözmek amacıyla, Sentetik Azınlık Aşırı Örneklem Tekniği (SMOTE ve Tomek bağlantıları (Tomek Links) birlikte kullanılmıştır. SMOTE, azınlık sınıfa ait (güvensiz) örnekleri sentetik olarak çoğaltarak sınıf dengesizliğini azaltırken; Tomek bağlantıları, birbirine çok yakın fakat farklı sınıflara ait

örnek çiftlerini tespit ederek sınıflar arası karışıklığı azaltır ve daha net karar sınırları elde edilmesini sağlar. Bu iki yöntemin birleşimi olan SMOTE-Tomek, modelin özellikle azınlık sınıfa (vulnerable functions) dair öğrenme başarımını artırarak genel sınıflandırma doğruluğunu iyileştirmeyi hedeflemiştir.

Tablo 2. Türetilen özellikler

Özellik Kodu	Açıklama
CYCLE_DENS_LOC	CYCL_DENS / LOC oranı, fonksiyonun satır başına döngüsel karmaşıklık yoğunluğunu gösterir.
HBUGS_LOC	HBUGS / LOC oranı, fonksiyonun satır başına hata oranını gösterir.
HBUGS_NOS	HBUGS / NOS oranı, fonksiyonun ifade başına hata oranını gösterir.
LOC_NOS	LOC / NOS oranı, fonksiyonun uzunluğunu ifade başına gösterir.
HBUGS_HDIFF	HBUGS / HDIFF oranı, yapılan değişiklikler başına hata oranını gösterir

3.4. Model Seçimi

Bu çalışmada, JavaScript kodlarında güvenlik açığı tespiti problemini farklı perspektiflerden ele alabilmek amacıyla 12 farklı makine öğrenmesi algoritması değerlendirilmiştir. Bu modeller;

- Doğrusal sınıflandırıcılar: Lojistik Regresyon (Logistic Regression), Destek Vektör Makineleri (SVM)
- Karar ağacı tabanlı yaklaşımlar: Rastgele Ormanlar (Random Forest; Breiman, 2001), Aşırı Gradyan Artırmalı Karar Ağaçları (XGBoost; Chen & Guestrin, 2016), LightGBM (Ke vd., 2017)
- İstatistiksel ve örnek tabanlı yöntemler: En Yakın

Komşu Algoritması (KNN – K-Nearest Neighbors), Naive Bayes (McCallum ve Nigam, 1998)

gibi çeşitli öğrenme paradigmalarını temsil etmektedir. Her modelin belirli avantajları bulunmakta olup, model performansları ve davranışları Bölüm 4.1’de detaylı olarak sunulmuştur.

3.5. Hiperparametre Optimizasyonu

Makine öğrenmesi modellerinin doğruluk, hassasiyet ve genellenebilirliğini artırmak amacıyla hiperparametre ayarları yapılmıştır. Bu kapsamda, geleneksel ızgara araması (grid search) gibi yöntemlere kıyasla daha az hesaplama maliyetiyle daha etkili sonuçlar sunan Bayes optimizasyonu (Snoek vd., 2012) tercih edilmiştir. Optimizasyon sürecinde, literatürde önerilen hiperparametre aralıkları kullanılmış ve her model için 50 iterasyonluk bir arama gerçekleştirilmiştir. Seçilen aralıklar ve dağılımlar, Tablo 3’te detaylı olarak verilmiştir.

3.6. Ensemble Yöntemleri

Modelin genel başarımını artırmak, farklı algoritmaların güçlü yönlerinden faydalanmak ve tekil modellerin zaafılarını dengelemek amacıyla iki farklı topluluk (ensemble) yöntemi uygulanmıştır:

- Voting Classifier: Birden fazla modelin tahminleri oy çokluğu ile birleştirilerek nihai karar verilir (Dietterich, 2000).
- Stacking Classifier: Birinci seviye öğrencilerden (base learners) elde edilen tahmin çıktıları, ikinci seviyedeki bir öğrenciye (meta-learner) giriş olarak verilerek daha kompleks karar mekanizması kurulmasını sağlar (Wolpert, 1992).

Bu yöntemlerin uygulanma adımları, doğrulama süreçleri ve elde edilen başarı metrikleri Bölüm 4.3’te kapsamlı şekilde sunulmuştur.

Tablo 3. Model hiperparametre aralıkları

Algoritma	Parametre	Aralık	Dağılım	Açıklama
KNN	n_neighbors	1 – 20	Uniform	Komşu sayısı
Random Forest	n_estimators	50 – 200	Uniform	Ağaç sayısı
	max_depth	5 – 30	Uniform	Ağaç derinliği
Gradient Boosting	n_estimators	50 – 200	Uniform	Boost sayısı
	learning_rate	0,01 – 0,3	Log-uniform	Öğrenme hızı
AdaBoost	n_estimators	50 – 200	Uniform	Ağırlıklı öğrenci sayısı
Bagging	n_estimators	10 – 200	Uniform	Bootstrap örnek sayısı
Extra Trees	n_estimators	10 – 200	Uniform	Rastgele ağaç sayısı
Logistic Regression	C	1e-6 – 1e+6	Log-uniform	Düzenleme katsayısı
SVM	C	1e-6 – 1e+6	Log-uniform	Margin kontrolü
Decision Tree	max_depth	3 – 30	Uniform	Ağaç derinliği
Naive Bayes	var_smoothing	1e-9 – 1e-5	Log-uniform	Sayısal kararlılık
XGBoost	n_estimators	50 – 200	Uniform	Boost sayısı
	learning_rate	0,01 – 0,3	Log-uniform	Öğrenme hızı
LightGBM	n_estimators	50 – 200	Uniform	Boost sayısı
	learning_rate	0,01 – 0,3	Log-uniform	Öğrenme hızı

4. Makine Öğrenme Modeli

Bu bölümde, JavaScript fonksiyonlarında güvenlik açıklarını tespit etmek amacıyla geliştirilen makine öğrenmesi tabanlı yaklaşımlar ayrıntılı olarak ele alınmaktadır. İlk olarak, sınıflandırma sürecinde kullanılan temel algoritmalar tanıtılmış; ardından veri setinin eğitime hazırlanması süreci açıklanmıştır. Son olarak, bireysel modellerin yanı sıra, doğruluk oranını artırmak amacıyla uygulanan Voting ve Stacking gibi topluluk (ensemble) öğrenme yöntemleri detaylı şekilde değerlendirilmiştir.

4.1. Kullanılan Modeller

Bu çalışmada tercih edilen makine öğrenmesi modelleri, farklı öğrenme paradigmalarını temsil edecek şekilde dikkatle seçilmiştir. Amaç, her bir modelin güçlü yönlerinden faydalanarak, güvenlik açığı tespiti gibi karmaşık bir problemi daha isabetli çözebilecek bir sistem oluşturmaktır.

Örneğin, Lojistik Regresyon (Logistic Regression) ve Destek Vektör Makineleri (SVM) gibi modeller doğrusal sınıflandırma yetenekleriyle bilinir. Lojistik Regresyon, verilerin lineer olarak ayrılabilirdiği durumlarda hızlı ve etkili sonuçlar sunarken (Hosmer ve Lemeshow, 2000; Şahin, 2025), SVM ise yüksek boyutlu uzayda karar sınırlarını optimize ederek ayırım performansını artırır (Cortes ve Vapnik, 1995).

Buna karşın, Karar Ağacı tabanlı modeller olan Rastgele Ormanlar (Random Forest; Breiman, 2001), XGBoost (Chen ve Guestrin, 2016) ve LightGBM (Ke vd., 2017), doğrusal olmayan ilişkileri modellemede oldukça başarılıdır. Özellikle Random Forest, overfitting riskini azaltan "bagging" stratejisi sayesinde yüksek varyansa sahip veri kümelerinde kararlı sonuçlar üretmektedir. XGBoost ve LightGBM ise boosting tabanlı yaklaşımlarıyla model hatalarını kademeli olarak azaltmakta ve yüksek doğruluk sağlamaktadır.

Diğer yandan, Naive Bayes gibi olasılıksal modeller, özellikler arasında koşulsuz bağımsızlık varsayımı ile çalışır (McCallum ve Nigam, 1998). Bu yöntem, özellikle metin sınıflandırma gibi alanlarda etkili olsa da, karmaşık bağımlılık ilişkilerini yakalamakta sınırlıdır. KNN gibi örnek-tabanlı algoritmalar ise, düşük boyutlu ve dengeli veri kümelerinde başarılı olmasına rağmen, yüksek boyut veya dengesiz sınıf dağılımlarında performans kaybı yaşayabilir.

Bu çeşitliliği avantaja çevirmek amacıyla bu çalışmada, ensemble yöntemleri olan Voting Classifier ve Stacking Classifier tercih edilmiştir. Ensemble yaklaşımlar, farklı modellerin karar mekanizmalarını birleştirerek genel hata oranını azaltmayı hedefler (Dietterich, 2000). Özellikle Stacking yöntemi, birinci seviye öğrencilerden (örneğin: ağaç tabanlı ve doğrusal modeller) elde edilen çıktıları ikinci bir öğrenciye (meta-learner) aktarır ve böylece modellerin birbirinin eksik yönlerini tamamlamasına olanak sağlar (Wolpert, 1992).

Burada "yatay" ve "dikey" katkılar kavramsallaştırması kullanılabilir: bazı modeller (örneğin karar ağaçları), verinin iç yapısını ayrıntılı biçimde çözümleyerek dikey

analiz yaparken; bazı modeller (örneğin Logistic Regression, SVM), daha genelleyici karar sınırları oluşturarak yüzeysel fakat geniş kapsamlı katkılar sağlar. Bu farklı stratejilerin bir araya getirilmesi, güvenlik açığı tespiti gibi çok boyutlu problemler için yüksek doğruluk ve genelleme kabiliyeti sunar.

Sonuç olarak, sistemde kullanılan modeller hem farklı karar stratejileri hem de farklı matematiksel temelleri ile birbirini tamamlamakta; bu da Stacking gibi yöntemlerin neden en yüksek başarıyı sağladığını açıklamaktadır (Wolpert, 1992).

4.2. Eğitime Hazırlık

Veri seti üzerinde yapılan ön işlemlerin ardından, sınıflandırma modellerinin performansını artırmak için hiperparametre optimizasyonu gerçekleştirilmiştir. Hiperparametreler, modelin öğrenme sürecinde ayarlanması gereken ve genel performansı doğrudan etkileyen parametrelerdir. Bu çalışmada, 12 farklı model için en uygun hiperparametreleri belirlemek amacıyla Bayes Arama (Bayesian Optimization) yöntemi kullanılmıştır. Bayes Arama, grid search ve rastgele arama (random search) yöntemlerinden farklı olarak, önceki denemelerden elde edilen bilgileri kullanarak arama alanını sistematik şekilde daraltır ve böylece optimal parametreleri daha hızlı ve etkili biçimde bulur (Snoek vd., 2012). Her model için belirlenen hiperparametre aralıkları Tablo 3'te sunulmuş olup, Bayes Arama yöntemi 50 iterasyon boyunca en iyi kombinasyonu aramıştır.

Hiperparametre optimizasyon sürecinde, her algoritma için anlamlı ve etkili olduğu bilinen hiperparametreler belirlenmiştir. Örneğin, $n\_neighbors$ parametresi yalnızca KNN modeli için uygulanabilirken, $n\_estimators$ parametresi Random Forest, XGBoost ve LightGBM gibi topluluk öğrenme (ensemble learning) modelleri için kritik öneme sahiptir. Parametre aralıkları, daha önce yapılan çalışmalar (Wolpert, 1992; Breiman, 2001; Chen ve Guestrin, 2016; Ke vd., 2017) ve ampirik gözlemler doğrultusunda belirlenmiş; dağılım türü ise parametrenin ölçeğine göre uniform ya da log-uniform olarak seçilmiştir.

Bayes optimizasyonu, 50 iterasyon boyunca bu hiperparametre uzayını tarayarak her model için en yüksek doğruluğu sağlayan kombinasyonu tespit etmiştir. Bu süreçte değerlendirme ölçütü olarak doğruluk (accuracy), hassasiyet (precision), duyarlılık (recall) ve F1 skoru dikkate alınmıştır.

4.3. Model Eğitimi

4.3.1. Voting classifier

Voting Classifier, birden fazla makine öğrenmesi modelinin tahminlerini birleştirerek nihai kararı verir (Dietterich, 2000). Bu çalışmada, KNN, Random Forest, Gradient Boosting, AdaBoost, Bagging, Extra Trees, Logistic Regression, SVM, Decision Tree, Naive Bayes, XGBoost ve LightGBM modelleri, SMOTE-Tomek ile dengelenmiş veri seti üzerinde eğitilmiştir. Her model için Bayes Arama yöntemiyle en iyi hiperparametreler belirlendikten sonra, bu modeller Voting Classifier içinde

bir araya getirilmiş, çapraz doğrulama yöntemiyle performansları değerlendirilmiş ve nihai model test veri seti üzerinde eğitilerek performans metrikleri (doğruluk, hassasiyet, duyarlılık ve F1 skoru) hesaplanmıştır. Voting Classifier, farklı modellerin güçlü yönlerini birleştirerek genel performansı artırmayı amaçlamakta olup, bu çalışmada hard voting yaklaşımı kullanılmıştır.

4.3.2. Stacking classifier

Stacking Classifier, birinci seviye öğrencilerin tahminlerini ikinci seviye öğrenciye (meta-öğrenci) aktararak nihai kararı verir (Wolpert, 1992). Bu çalışmada, KNN, Random Forest, Gradient Boosting, AdaBoost, Bagging, Extra Trees, Logistic Regression, SVM, Decision Tree, Naive Bayes, XGBoost ve LightGBM modelleri birinci seviye öğrenci olarak kullanılmış; SMOTE-Tomek ile dengelenmiş veri seti üzerinde eğitilmiştir. Birinci seviye modellerin tahminleri, ikinci seviye öğrenci olarak seçilen LightGBM'e aktarılmış; çapraz doğrulama yöntemiyle performans değerlendirilmiş ve test veri seti üzerinde nihai performans metrikleri hesaplanmıştır. Bu yöntem, farklı modellerin güçlü yönlerini birleştirerek daha yüksek doğruluk ve genelleme kapasitesi sağlamayı hedefler.

5. Bulgular

Bu bölümde model eğitimi aşaması sonrası kullanılan modelin doğrulama ve test işlemleri gerçekleştirilmiştir. Gerçekleştirilen testler sonucunda elde edilen sonuçlar karşılaştırmalı olarak verilmiştir.

5.1. Çapraz Doğrulama

Model doğrulama sürecinde, veri seti 5 katlı Stratified K-Fold yöntemiyle eşit parçalara bölünmüş ve her fold sırayla test seti olarak kullanılmıştır. Bu yöntem, sınıf dağılımını dengeli tutarken, cross_val_score fonksiyonu ile modelin doğruluk (accuracy) skorunu hesaplamayı sağlamıştır. Voting ve Stacking Classifier modelleri için uygulanan bu çapraz doğrulama sonucunda, modelin genel performansını yansıtan ortalama doğruluk skoru 0,9397 elde edilmiştir.

5.2. Test Performansı

Model eğitimi ve doğrulama tamamlandıktan sonra, eğitimde kullanılmayan test veri seti üzerinde modellerin performansı değerlendirildi. Voting ve Stacking Classifier modelleri, SMOTE-Tomek ile dengelenmiş eğitim verisiyle eğitildikten sonra, test veri setinde tahminlerde bulunarak doğruluk (accuracy), hassasiyet (precision), duyarlılık (recall) ve F1 skoru gibi metrikler hesaplandı. Tablo 4'de verilen tüm model performansları değerlendirildiğinde, Extra Trees modeli en yüksek doğruluk oranını sağlamıştır. Bu modelin doğruluğu 0,9694 olarak hesaplanmıştır.

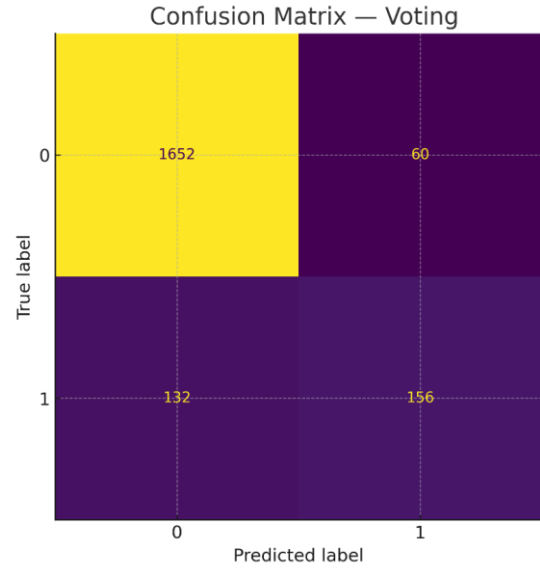
Confusion matrix (karmaşıklık matrisi), modelin doğru ve yanlış sınıflandırmalarını görselleştirmek için kullanılır. Bu matris, gerçek sınıflar ile modelin tahmin ettiği sınıflar arasındaki ilişkiyi gösterir.

Şekil 2'de gösterilen karmaşıklık matrisinde, Voting Classifier modelinin yüksek doğruluk oranına sahip olduğunu görülmektedir. Model, negatif ve pozitif

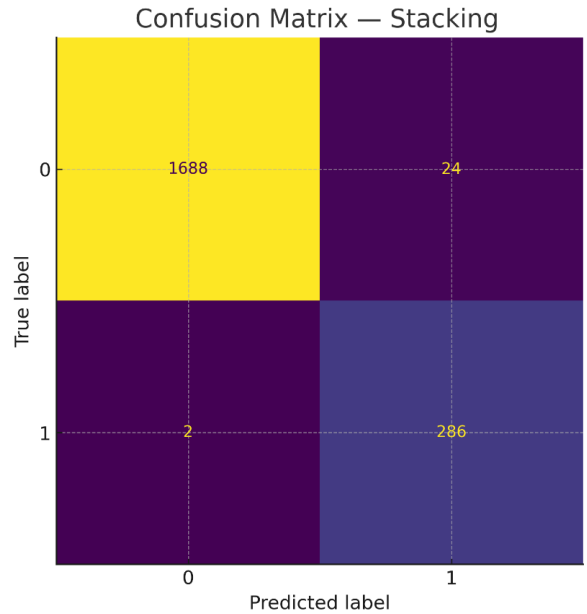
sınıfları büyük ölçüde doğru sınıflandırırken, düşük yanlış pozitif (FP) değeriyle yanlış alarm üretme olasılığını minimize etmiştir. Ancak, nispeten yüksek yanlış negatif (FN) değeri, bazı pozitif örneklerin hatalı sınıflandırıldığını göstermektedir.

Tablo 4. Model performans sonuçları

Metric	Voting Classifier	Stacking Classifier
Accuracy	0,9495	0,9751
Precision	0,9736	0,9755
Recall	0,9227	0,9741
F1 Score	0,9475	0,9748



Şekil 2. Voting classifier için karmaşıklık matrisi.



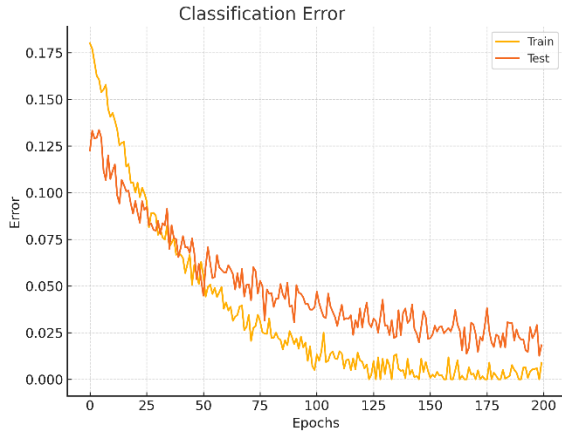
Şekil 3. Stacking classifier için karmaşıklık matrisi.

Şekil 3'te Stacking Classifier için oluşturulan karmaşıklık matrisi verilmiştir. Model, oldukça başarılı bir performans göstermektedir. Özellikle FN değerinin oldukça düşük olması, modelin pozitif örnekleri kaçırma oranının çok az olduğunu göstermektedir. FP değeri de

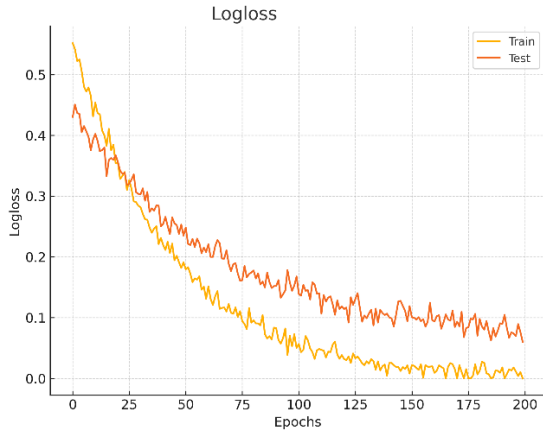
düşük olduğu için model yanlış alarm üretme konusunda da başarılıdır. Genel olarak, Stacking Classifier modeli Voting Classifier' a kıyasla daha yüksek doğruluk ve daha düşük hata oranları ile daha iyi bir performans sergilemektedir.

Şekil 4, Eğitim ve doğrulama hataları dönem boyunca düzenli biçimde azalmakta; iki eğri birbirine yakın seyrettiği için belirgin bir ayrışma (overfitting) gözlenmemektedir. Bu durum, modelin öğrenirken genelleme kabiliyetini koruduğunu gösterir.

Şekil 5, Her iki logloss eğrisi de istikrarlı şekilde düşmektedir ve doğrulama eğrisi yukarı yönlü sapma göstermemektedir. Bu, olasılık tahminlerinin giderek daha iyi kalibre olduğunu ve modelin eğitim sürecinin sağlıklı ilerlediğini ortaya koyar.

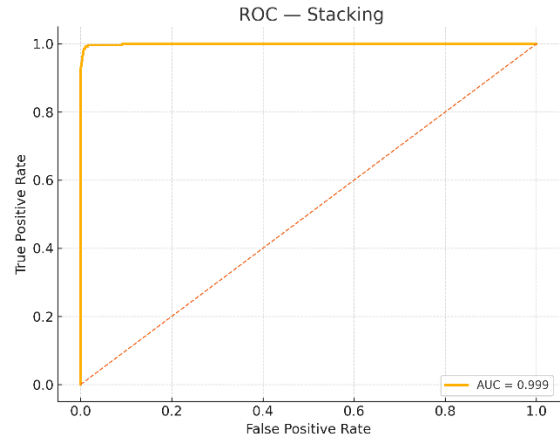


Şekil 4. Eğitim ve doğrulamahata oranı (epoch).

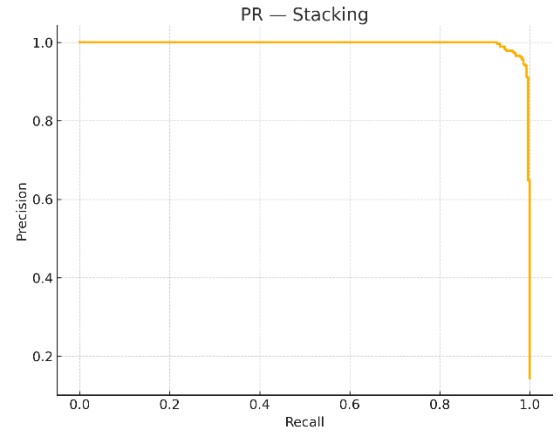


Şekil 5. Eğitim ve doğrulama logloss (epoch).

Şekil 6 ve Şekil 7 Stacking Classifier için ROC ve PR eğrileri. ROC (Receiver Operating Characteristic) eğrisi, modelin yanlış pozitif oranı (False Positive Rate) ile doğru pozitif oranı (True Positive Rate) arasındaki ilişkiyi göstererek sınıflandırma performansını ölçer. Eğrinin altında kalan alan (AUC – Area Under Curve) değeri ne kadar 1'e yakınsa, modelin genel performansı o kadar iyidir. Bu çalışmada Stacking Classifier modeli için elde edilen AUC değeri 0,99 seviyesindedir, bu da modelin hem pozitif hem negatif sınıfları ayırt etme kabiliyetinin yüksek olduğunu göstermektedir.



Şekil 6. ROC eğrisi.



Şekil 7. PR eğrisi.

PR (Precision-Recall) eğrisi ise özellikle dengesiz veri setlerinde daha anlamlı bir değerlendirme sunar. Bu eğri, modelin doğru pozitif oranını (recall) ve yanlış alarm üretmeden ne kadar doğru tahmin yaptığını (precision) görselleştirir. Elde edilen PR eğrisinin yüksek bir eğimde ve geniş alanda seyretmesi, modelin pozitif sınıfı doğru şekilde tahmin ederken aynı zamanda düşük oranda yanlış alarm ürettiğini göstermektedir.

Bu grafikler, Stacking Classifier modelinin özellikle azınlık (vulnerable) sınıfı doğru tahmin etmedeki başarısını kanıtlamakta ve çalışma kapsamında uygulanan ensemble yaklaşımının etkinliğini desteklemektedir.

6. Tartışma ve Sonuç

Bu çalışmada, JavaScript programlama dili içerisinde yer alan fonksiyonların güvenlik açıklarını tespit edebilmek amacıyla JSVULNDETECT adlı makine öğrenmesi tabanlı bir sistem geliştirilmiştir. Sistem, statik analiz teknikleri kullanarak fonksiyonlardan çıkarılan özellikler üzerinden güvenli/güvensiz sınıflandırması yapmakta ve bu süreci otomatikleştirerek hem zamandan tasarruf sağlamakta hem de insan hatasını minimize etmektedir.

Model geliştirme sürecinde karşılaşılan sınıf dengesizliği problemi, SMOTE-Tomek yöntemi ile etkin biçimde çözülmüş, bu sayede azınlık sınıf olan “güvensiz fonksiyonlar” için sınıflandırma başarımı artırılmıştır.

Ayrıca, her biri farklı öğrenme stratejilerine sahip 12 makine öğrenimi modeli hiperparametre optimizasyonu ile değerlendirilmiş ve bu kapsamda Bayesian Search yaklaşımı kullanılmıştır. Voting ve Stacking gibi ensemble öğrenme teknikleri sayesinde model performansı daha da artırılmış ve özellikle Stacking Classifier modeli ile %97,51 doğruluk oranı elde edilmiştir.

Geliştirilen sistem, yalnızca yüksek doğrulukla sınıflandırma yapmakla kalmamış, aynı zamanda önceki literatür çalışmalarının ötesine geçerek çok sayıda modelin karşılaştırmalı analizini sağlamıştır. Örneğin Ferenc vd. (2019) çalışmasında yalnızca birkaç temel model kullanılarak daha düşük doğruluklar elde edilmişken, bu çalışmada kapsamlı modelleme yaklaşımı ve optimizasyon süreci sayesinde daha güçlü sonuçlar alınmıştır. Bu durum, önerilen sistemin hem teknik hem de yöntemsel açıdan literatüre anlamlı bir katkı sunduğunu ortaya koymaktadır.

Ayrıca, JSVULNDETECT sisteminin web tabanlı bir arayüzle erişilebilir olması, onu sadece akademik araştırmalar için değil, aynı zamanda gerçek dünya uygulamaları için de uygun hale getirmektedir. Sistem, yazılım geliştiriciler ve güvenlik uzmanları için kullanılabilir bir araç olarak işlev görmektedir.

Bu çalışma kapsamında sunulan temel katkılar aşağıda özetlenmiştir:

- Güvenlik açığı tespitinde çok modellerli yaklaşım ve hiperparametre optimizasyonunun birlikte uygulanması,
- SMOTE-Tomek ile veri dengesizliği probleminin çözülmesi ve bunun model başarımı üzerindeki etkisinin gösterilmesi,
- Kullanıcı dostu web arayüzü ile geliştiricilere pratik kullanım imkânı sunan bir sistem tasarımı,
- Güvenlik alanında açıklanabilirlik ve genellenebilirlik açısından örnek teşkil edecek açık ve sistematik bir yaklaşımın sunulması.

Gelecek çalışmalarda sistemin kapsamı ve etkinliği daha da artırılabilir. Öncelikli olarak, GitHub gibi açık kaynaklı platformlardan elde edilecek daha güncel ve çeşitli JavaScript projeleri ile veri setinin genişletilmesi, modelin genelleme yeteneğini ve farklı güvenlik senaryolarına adaptasyon kabiliyetini güçlendirecektir. Ayrıca sistemin yalnızca JavaScript ile sınırlı kalmaksızın Python, PHP ve Ruby gibi farklı programlama dillerini de kapsayacak şekilde genişletilmesi, çok dilli güvenlik analizi için önemli bir adım olacaktır. Bununla birlikte, mevcut sistem statik analiz temelli çalışmakta olup, ilerleyen süreçte dinamik analiz teknikleriyle desteklenmesi; özellikle çalışma zamanında ortaya çıkan saldırgan davranışların tespiti açısından fayda sağlayacaktır. Modelin karar verme süreçlerini şeffaflaştırmak amacıyla SHAP ve LIME gibi açıklanabilir yapay zeka (XAI) yöntemlerinin entegrasyonu planlanmakta; böylece kullanıcıya hangi özelliklerin hangi güvenlik risklerine yol açtığı daha anlaşılır biçimde sunulabilecektir. Son olarak, geliştirilecek sistemin RESTful API mimarisi ile yapılandırılarak sürekli

entegrasyon/sürekli dağıtım (CI/CD) süreçlerine, yaygın kullanılan geliştirme ortamlarına (örneğin Visual Studio Code) veya tarayıcı uzantılarına entegre edilmesi hedeflenmektedir. Bu sayede geliştiricilerin gerçek zamanlı güvenlik uyarıları alabilmesi ve yazılım yaşam döngüsü boyunca güvenlik farkındalığının artırılması mümkün olacaktır.

Bu çalışma, yazılım güvenliği alanında hem teknik hem de pratik açıdan güçlü bir çözüm sunmakta; özellikle yazılım geliştirme sürecine güvenlik perspektifini dahil etmek isteyen araştırmacı ve profesyoneller için yenilikçi bir yaklaşım ortaya koymaktadır.

Katkı Oranı Beyanı

Yazarların katkı yüzdeleri aşağıda verilmiştir, Yazarlar makaleyi incelemiş ve onaylamıştır.

%	H.H.A.	Ö.T.	Z.C.
K	50	50	
T	50	50	
Y	40	30	30
VTI		50	50
VAY	100		
KT	50	50	
YZ	100		
GR		50	50
PY		50	50

K= kavram, T= tasarım, Y= yönetim, VTI= veri toplama ve/veya işleme, VAY= veri analizi ve/veya yorumlama, KT= kaynak tarama, YZ= Yazım, GR= gönderim ve revizyon, PY= proje yönetimi.

Çalışma Beyanı

Yazarlar bu çalışmada hiçbir çıkar ilişkisi olmadığını beyan etmektedirler.

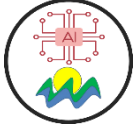
Etik Onay Beyanı

Bu araştırmada hayvanlar ve insanlar üzerinde herhangi bir çalışma yapılmadığı için etik kurul onayı alınmamıştır.

Kaynaklar

- Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5–32. <https://doi.org/10.1023/A:1010933404324>
- Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785–794). <https://doi.org/10.1145/2939672.2939785>
- Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning*, 20(3), 273–297. <https://doi.org/10.1007/BF00994018>
- Dietterich, T. G. (2000). Ensemble methods in machine learning. In J. Kittler & F. Roli (Eds.), *Multiple Classifier Systems* (pp. 1–15). Springer. https://doi.org/10.1007/3-540-45014-9_1
- Ferenc, R., Hegedűs, P., Gyimesi, P., Antal, G., Bán, D., & Gyimóthy, T. (2019). Challenging machine learning algorithms in predicting vulnerable JavaScript functions. In *2019 IEEE/ACM 7th International Workshop on Realizing Artificial Intelligence Synergies in Software Engineering (RAISE)* (pp. 8–14). IEEE. <https://doi.org/10.1109/RAISE.2019.00010>
- Friedman, J. H. (2001). Greedy function approximation: A

- gradient boosting machine. *The Annals of Statistics*, 29(5), 1189–1232. <https://doi.org/10.1214/aos/1013203451>
- Geurts, P., Ernst, D., & Wehenkel, L. (2006). Extremely randomized trees. *Machine Learning*, 63(1), 3–42. <https://doi.org/10.1007/s10994-006-6226-1>
- Harzevili, N. S., Belle, A. B., Wang, J., Wang, S., Jiang, Z. M., & Nagappan, N. (2023). *A survey on automated software vulnerability detection using machine learning and deep learning* (arXiv:2306.11673). arXiv. <https://doi.org/10.48550/arXiv.2306.11673>
- Hosmer, D. W., & Lemeshow, S. (2000). *Applied logistic regression* (2nd ed.). John Wiley & Sons.
- Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., & Liu, T. Y. (2017). LightGBM: A highly efficient gradient boosting decision tree. *Advances in Neural Information Processing Systems*, 30, 3146–3154. <https://proceedings.neurips.cc/paper/2017/file/6449f44a102fde848669bdd9eb6b76fa-Paper.pdf>
- Liu, Z., Fang, Y., Huang, C., & Xu, Y. (2023). MFXSS: An effective XSS vulnerability detection method in JavaScript based on multi-feature model. *Computers & Security*, 124, 103015. <https://doi.org/10.1016/j.cose.2022.103015>
- McCallum, A., & Nigam, K. (1998). A comparison of event models for naive Bayes text classification. In *AAAI-98 Workshop on Learning for Text Categorization* (pp. 41–48). AAAI Press.
- Şahin, M. (2025). Binary logistic regression procedure with an application. *Black Sea Journal of Statistics*, 1(1), 22–26. <https://blackseapublishers.online/index.php/statistics/article/view/21>
- Snoek, J., Larochelle, H., & Adams, R. P. (2012). Practical Bayesian optimization of machine learning algorithms. *Advances in Neural Information Processing Systems*, 25, 2951–2959.
- Wolpert, D. H. (1992). Stacked generalization. *Neural Networks*, 5(2), 241–259. [https://doi.org/10.1016/S0893-6080\(05\)80023-1](https://doi.org/10.1016/S0893-6080(05)80023-1)



VERİ OKURYAZARLIĞINDAN YAPAY ZEKÂYA: DİJİTAL ÇAĞIN ELEŞTİREL YETKİNLİKLERİ ÜZERİNE BİR DERLEME

Engin DAYAN^{1*}

¹Iğdır University, Vocational School of Health Services, 76200, Iğdır, Türkiye

Özet: Bu derleme çalışması, 2010–2025 yılları arasında yayımlanan akademik literatür ışığında veri okuryazarlığı ile yapay zekâ (YZ) okuryazarlığı arasındaki ilişkiyi incelemektedir. Çalışmanın amacı, bu iki kavramın kesişim noktalarını, birbirini nasıl tamamladığını ve dijital çağda bireyler ile kurumlar için taşıdığı önemi analiz etmektir. Dijitalleşmenin hız kazandığı günümüzde, bireylerin ve kurumların veriye dayalı karar alma, algoritmik sistemleri anlama ve etik farkındalık geliştirme becerileri, hem veri okuryazarlığı hem de yapay zekâ okuryazarlığı kavramlarının kapsamını genişletmiştir. Çalışma, özellikle eğitim ortamlarında ve kullanıcı odaklı YZ uygulamalarında bu iki kavramın etkileşimlerini değerlendirmektedir. Literatürde yapay zekâ okuryazarlığının yalnızca teknik bilgi ile sınırlı olmadığı; aynı zamanda eleştirel düşünme, etik duyarlılık ve şeffaflık gibi becerileri de kapsadığı görülmektedir. Ayrıca yapay zekâ sistemlerinin çıktıların doğru anlaşılabilmesi ve güvenli biçimde kullanılabilmesi için bireylerin güçlü bir veri okuryazarlığına sahip olmaları gerektiği vurgulanmaktadır. Çalışma, YZ çağında bireylerin ve toplumların dijital okuryazarlık düzeylerinin artırılması için bütüncül eğitim politikalarına ve ölçme araçlarına duyulan ihtiyacı ortaya koymaktadır.

Anahtar kelimeler: Bilgi okuryazarlığı, Veri okuryazarlığı, Yapay zeka okuryazarlığı, Bilgiye erişim sistemleri

From Data Literacy to Artificial Intelligence: A Review of Critical Competencies in the Digital Age

Abstract: This review study explores the relationship between data literacy and artificial intelligence (AI) literacy, based on academic literature published between 2010 and 2025. The aim of the study is to analyze the intersections between these two concepts, how they complement each other, and their significance for individuals and institutions in the digital age. As digitalization accelerates, the ability of individuals and institutions to make data-driven decisions, interpret algorithmic systems, and develop ethical awareness has expanded the scope of both data literacy and AI literacy. The study focuses on the intersection of these two literacies, particularly in educational settings and user-centered AI applications. The literature shows that AI literacy goes beyond technical knowledge, encompassing critical thinking, ethical sensitivity, and transparency. Moreover, it emphasizes that individuals need strong data literacy skills to understand and use AI systems effectively and responsibly. This study highlights the need for comprehensive educational policies and assessment tools to enhance digital literacy competencies in the age of AI.

Keywords: Information literacy, Data literacy, AI literacy, Information access systems

*Sorumlu yazar (Corresponding author): Iğdır University, Vocational School of Health Services, 76200, Iğdır, Türkiye

E mail: engin.dayan065@gmail.com (E. DAYAN)

Engin DAYAN <https://orcid.org/0000-0003-1839-280X>

Gönderi: 10 Mayıs 2025

Kabul: 23 Mayıs 2025

Yayınlanma: 15 Haziran 2025

Received: May 10, 2025

Accepted: May 23, 2025

Published: June 15, 2025

Cite as: Dayan, E. (2025). From data literacy to artificial intelligence: A review of critical competencies in the digital age. *Black Sea Journal of Artificial Intelligence*, 1(1), 25–30.

1. Giriş

Dijital teknolojilerin hızlı gelişimi, bilgi üretimi ve erişimi süreçlerini dönüştürürken, bireylerin bu yeni bilgi ortamlarında etkin rol alabilmeleri için sahip olmaları gereken beceri setlerini de yeniden tanımlamaktadır. Artık yalnızca bilgiye ulaşmak yeterli görülmemekte; bu bilginin nasıl üretildiği, nasıl yapılandırıldığı, nasıl sunulduğu ve ne tür toplumsal etkiler doğurduğu gibi daha derin sorular da gündeme gelmektedir. Bu bağlamda veri okuryazarlığı ve yapay zekâ (YZ) okuryazarlığı, bireylerin dijital ortamda bilinçli kullanıcılar ve eleştirel düşünürler olarak konumlanmaları açısından temel öneme sahiptir (Pangrazio ve Selwyn, 2021; Pinski ve Benlian, 2024). Veri okuryazarlığı, bireylerin verileri anlama, değerlendirme, analiz etme ve bu verilere dayanarak

karar verme yetilerini kapsayan çok katmanlı bir yeterlilik alanıdır. Ancak bu yetkinlik yalnızca teknik araç bilgisiyle sınırlı değildir; verilerin hangi bağlamda üretildiği, ne tür varsayımlara dayandığı, hangi aktörlerin kontrolünde olduğu gibi etik ve eleştirel soruları da içerir. Bu yönüyle veri okuryazarlığı, bilgi biliminin temel tartışma alanlarından biri olan bilgiye eleştirel yaklaşımı içselleştirir (Pangrazio ve Selwyn, 2021).

Benzer biçimde, yapay zekâ okuryazarlığı da giderek genişleyen bir içerik yapısına sahiptir. İlk dönem çalışmalar YZ okuryazarlığını algoritmaları tanıma, sistemlerin nasıl çalıştığını temel düzeyde kavrama gibi teknik bilgi ekseninde ele alırken; son yıllarda yapılan derinlikli çalışmalar, bu kavramın aynı zamanda etik farkındalık, algoritmik önyargıların tanınması, şeffaflık beklentisi ve toplumsal etkileri değerlendirme gibi



alanları da kapsadığını göstermektedir (Almatrafi vd., 2024; Gu ve Ericson, 2025). Özellikle üretken yapay zekâ teknolojilerinin (örneğin dil modelleri ve üretici sistemler) yaygınlaşmasıyla birlikte bu okuryazarlık türü, kullanıcıların sadece “nasıl kullanacağını” değil, “nasıl anlayacağını ve sorgulayacağını” da içeren eleştirel bir çerçeveye evrilmiştir.

Eğitim, kamu politikaları, iş dünyası ve kütüphane hizmetleri gibi pek çok alanda YZ destekli sistemlerin kullanımı artarken, bireylerin bu teknolojilere yalnızca tüketici olarak değil, aynı zamanda bilinçli ve sorumlu kullanıcılar olarak katılması da önem kazanmaktadır. Yapay zekâ uygulamalarının karar süreçlerine entegre edildiği ortamlarda, bireylerin veri okuryazarlığı düzeyleri, YZ sistemlerinden elde edilen sonuçları yorumlama ve sorgulama kapasitelerini doğrudan etkilemektedir (Mills vd., 2024). Bu durum, veri okuryazarlığı ile yapay zekâ okuryazarlığı arasındaki ilişkinin yalnızca kavramsal değil, aynı zamanda pratik ve işlevsel düzeyde de ne kadar iç içe geçtiğini göstermektedir.

Bu derleme çalışmasının amacı, 2010–2025 yılları arasında yayımlanmış güncel akademik çalışmalara dayanarak, veri okuryazarlığı ile yapay zekâ okuryazarlığı arasındaki ilişkiyi bilgi bilimi perspektifinden değerlendirmektir. Çalışmada, söz konusu okuryazarlık biçimlerinin tanımları, bileşenleri, ölçüm araçları, eğitim stratejileri ve etik yönleri analiz edilerek, aralarındaki kesişim alanları ve karşılıklı etkileşimleri ortaya konulmaktadır. Böylelikle dijital çağda bireylerin ve toplumların bu iki temel yetkinlik üzerinden nasıl güçlendirilebileceği tartışılacaktır.

2. Materyal ve Yöntem

Bu çalışma, 2010–2025 yılları arasında yayımlanmış akademik çalışmaları esas alarak yapılandırılmış bir derleme yöntemiyle yürütülmüştür. Literatür taraması kapsamında Web of Science, Scopus, ERIC ve Google Scholar veri tabanları kullanılmıştır. Tarama, “veri okuryazarlığı”, “YZ okuryazarlığı”, “eleştirel veri okuryazarlığı” ve “dijital okuryazarlık” gibi anahtar kelimelerle yürütülmüş ve tam metin yayınlar değerlendirmeye alınmıştır. Çalışmaların seçiminde şu kriterler dikkate alınmıştır:

- Yayın tarihi: 2010–2025
- İçerik: Veri okuryazarlığı, YZ okuryazarlığı, dijital okuryazarlık veya kütüphaneler ile ilişkili olması
- Tür: Derleme, özgün araştırma, vaka çalışması, metodolojik model veya kavramsal analiz

Toplamda 60’tan fazla akademik yayın taranmış; içeriği doğrudan çalışma amacını karşılayan 20 nitelikli yayın detaylı incelemeye dahil edilmiştir. Veriler betimsel ve tematik analiz yaklaşımıyla değerlendirilmiş; ortak kavramlar, eğilimler ve metodolojik boşluklar belirlenmiştir.

3. Veri Okuryazarlığı Nedir?

Veri okuryazarlığı, bireylerin modern bilgi ortamlarında veriyle etkileşimde bulunma, veri okuma, anlama, yorumlama ve karar alma becerilerini kapsayan çok boyutlu bir yetkinlik alanıdır. Dijital çağda, kişisel ve toplumsal verilerin hızla artmasıyla birlikte, veri okuryazarlığı bireylerin dijital ortamda bilinçli ve etkili bir şekilde hareket etmeleri için kritik bir öneme sahiptir. Bilgi bilimi perspektifi, bu kavramı yalnızca teknik yetkinliklerle sınırlı görmeyip, aynı zamanda veriyi etik, eleştirel ve kültürel bir bağlamda ele almanın önemine vurgu yapar (Calzada Prado ve Marzal, 2013; Pangrazio ve Selwyn, 2021). Bu bağlamda, veri okuryazarlığı, dijital platformların özelliklerine göre farklı beceri ve yaklaşımları içeren beş temel formda ele alınabilir (Tablo 1).

Tablo 1. Veri okuryazarlığına yönelik yaklaşımlar

Yaklaşım	Açıklama
Bilgi Erişimi ve Yönetimi	Veriye erişim, düzenleme, depolama ve yönetim yöntemleri
Veri Güvenliği	Dijital gizlilik, ayar yönetimi, sosyal veri paylaşım güvenliği
Veri Bilimi Odaklı Yaklaşım	Açık veri analizi, istatistik, veri görselleştirme
Veri Hacking	Veriyi yapısal olarak çözme, yeniden kullanım, hack etkinlikleri
Eleştirel Veri Yaklaşımı	Veri politikaları, ideoloji, etik kullanım, bilgi adaleti sorguları

İlk olarak, bilgi erişimi ve yönetimi boyutu, bireylerin veriyi nasıl bulduklarına, hangi kaynaklardan erişim sağladıklarına ve veriyi nasıl düzenleyip yönettiklerine odaklanır. Calzada Prado ve Marzal (2013), veri okuryazarlığını “bilgi okuryazarlığının, veriye erişim, yorumlama, eleştirel değerlendirme ve etik kullanım boyutlarını içeren bir bileşeni” olarak tanımlamışlardır.

İkinci olarak, veri güvenliği yaklaşımı kişisel gizlilik ve dijital güvenlik bilinciyle ilgilidir. Bireylerin sosyal medya gibi dijital ortamlarda bıraktıkları izleri kontrol edebilmesi, gizlilik ayarlarına hâkim olması önemlidir. Bu yaklaşım genellikle çocuklar, gençler ve aileler için sosyal verilerin paylaşımı ve güvenli kullanımı yönünde eğitici programlar biçiminde sunulur. Bu bağlamda, bireylerin açık veri kümeleriyle çalışabilmeleri, temel istatistiksel analizleri gerçekleştirebilmeleri ve veri görselleştirme araçlarını kullanabilmeleri beklenmektedir.

Üçüncü önemli boyut, veri bilimi odaklı okuryazarlıktır. Dünya Bankası gibi kurumlar tarafından yürütülen “Data Boot Camp” örneklerinde olduğu gibi, bireylerin açık veri setleri üzerinde temel istatistiksel analizler yapabilmesi ve çıkarımlar üretebilmesi beklenir. Bu teknik yaklaşım, veri bilimini veri okuryazarlığına dahil eden kapsamlı bir model önerisidir (Dhar, 2013).

Alternatif bir yaklaşım olarak “veri hacking” ya da “veri ile yaratıcı müdahale” söylemi de son yıllarda dikkat

çekmektedir. Bu yaklaşım, yalnızca veriyi kullanmakla kalmayıp aynı zamanda onun yapısını çözümlemeyi, sistemleri sorgulamayı ve gerektiğinde yeniden düzenlemeyi kapsar. Özellikle programcı topluluklarında görülen bu yaklaşım, toplumsal eşitsizliklere karşı dijital araçlarla çözüm üretme potansiyelini taşımaktadır (Boyd, 2014).

Son olarak, eleştirel veri okuryazarlığı, veri üretiminin toplumsal, kültürel ve ideolojik boyutlarını sorgulamayı içerir. Pangrazio ve Selwyn (2021) veriyi sömürselleştirme süreçlerine, algoritmik önyargılara ve bilgi adaletsizliğine yönelik farkındalığın geliştirilmesi gerektiğini vurgular. Bu yaklaşım, özellikle dijital vatandaşlık, platform kapitalizmi ve algoritmik önyargılar gibi kavramlarla yakından ilişkilidir.

Sonuç olarak, veri okuryazarlığı farklı alanlar tarafından farklı şekillerde tanımlansa da ortak payda, bireylerin veriye yalnızca teknik bir nesne olarak değil, toplumsal, etik ve eleştirel bir çerçevede yaklaşımlarının gerekliliğidir. Bilgi bilimi disiplini bu çerçevede, veriyle kurulan ilişkinin hem bilişsel hem de etik boyutlarını bir arada ele alan bütüncül bir bakış açısı sunmaktadır.

4. Yapay Zekâ (AI) Okuryazarlığı

Yapay zekâ (YZ), günümüzde kullanıcıların sıklıkla etkileşimde bulunduğu teknolojilerde giderek daha fazla entegre bir hale gelmektedir. YZ teknolojilerinin sağlık, eğitim, ulaşım ve eğlence gibi çeşitli sektörlerde yaygınlaşması, YZ okuryazarlığını kritik bir beceri haline getirmiştir. Yim (2024)'e göre, YZ okuryazarlığı, bireylerin YZ sistemlerinin benimsenmesi ve hesap verebilirliği hakkında eleştirel düşüncelerini sağlar ve ulusal rekabet, iş gücü hazırlığı ve çevrimiçi güvenlik açısından hayati öneme sahiptir.

Kullanıcılar çoğu zaman bir algoritmayla karşı karşıya olduklarının farkında olmadan bu sistemleri kullanmakta; bu da bireylerin YZ'ya ilişkin yanlış anlamalar geliştirmelerine neden olmaktadır (Eslami vd., 2015; Eslami vd., 2019). Ayrıca, YZ'yı etkili bir şekilde kullanma, iş birliği yapma ve eleştirel bir tüketici olarak hareket etme yeteneklerini sınırlayabilmektedir. Bu yanlış anlamalar ile ayrıca, düzenleyici müdahalelerin yanlış yönlendirilmesine ve kamuoyunda hayal kırıklığına yol açabilmektedir (Fast ve Horvitz, 2017; Stone vd., 2022). Bu bağlamda, yapay zekâ okuryazarlığı, bireylerin YZ teknolojilerini eleştirel bir şekilde değerlendirmelerini, etkili bir şekilde iletişim kurmalarını ve iş birliği yapmalarını, ayrıca YZ'yı çevrimiçi ortamda, evde ve iş yerinde bir araç olarak kullanmalarını sağlayan bir dizi yetkinlik olarak tanımlanabilir.

Son yıllarda İnsan-Bilgisayar Etkileşimi (HCI) araştırmacıları, YZ'yı halkın nasıl algıladığını incelemekte ve daha anlaşılır sistemler tasarlamak için çalışmalar yürütmektedir (Druga vd., 2017; Gunning, 2017). Ancak YZ'nın bireylerin iletişim kurma, çalışma ve birlikte yaşama biçimlerini dönüştüreceği bir gelecekte, bireylerin hangi yeni yetkinliklere ihtiyaç duyacağına

yönelik kapsamlı araştırmalara hâlâ ihtiyaç vardır. Bu bağlamda geliştirilen YZ okuryazarlığı (AI literacy) kavramı, bu yeni yeterlilikleri tanımlamak üzere ortaya çıkmaktadır.

YZ okuryazarlığını geliştirmeye yönelik çalışmalar özellikle teknik altyapısı olmayan bireyleri hedeflemektedir. Örneğin, son dönemde bazı teknoloji şirketleri, YZ eğitiminin farklı gruplara yayılmasını sağlamak ve iş gücünde çeşitliliği artırmak amacıyla yeni girişimlerde bulunmuştur. Eğitimciler, K-12 düzeyinde yapay zekânın müfredata entegrasyonu için rehberler yayımlamış; araştırmacılar ise çocukların YZ ile yaratıcı biçimde programlama etkinliklerine katılmasını sağlamak üzere projeler geliştirmiştir (Kahn ve Winters, 2017; Zimmerman, 2018; Long ve Magerko, 2020).

Bu çabaların merkezinde yer alan "AI for K-12" çalışma grubu, sınıf içi uygulamalar için beş temel kavram tanımlamıştır, bunlar (Touretzky vd., 2019):

- Bilgisayarlar dünyayı sensörler aracılığıyla algılar,
- Ajanlar dünya hakkında temsiller/modellemeler geliştirir ve bunlarla akıl yürütür,
- Bilgisayarlar veriden öğrenebilir,
- İnsanlarla etkileşim kurmak YZ geliştiricileri için temel bir zorluktur,
- YZ uygulamaları toplumu hem olumlu hem de olumsuz yönde etkileyebilir.

Bu temel ilkeler, teknik olmayan bireyler için de erişilebilir bir YZ okuryazarlığı çerçevesi sunmaktadır. Web araştırmaları, bu yetkinliklerin, bireylerin YZ sistemlerini güvenli ve etkili bir şekilde kullanmalarını sağladığını ve etik farkındalığı artırdığını göstermektedir (Digital Promise, 2024).

YZ okuryazarlığı kavramı, dijital, hesaplamalı, bilimsel ve veri okuryazarlığı gibi daha önce tanımlanmış okuryazarlık türleriyle yakından ilişkilidir. Dijital okuryazarlık, kullanıcıların bilgisayarı etkin bir şekilde kullanabilmesi bakımından bir ön koşul olarak kabul edilirken, hesaplamalı okuryazarlık (örneğin kod yazma bilgisi) gerekli görülmemektedir. Bilimsel okuryazarlık, özellikle makine öğrenmesi süreçlerini anlamada faydalı olabilir (Shapiro vd., 2018 ; Long ve Magerko, 2020) . Ancak zorunlu bir ön bilgi değildir. Diğer yandan, veri okuryazarlığı ise özellikle makine öğrenmesi alanında doğrudan örtüşen yetkinlikleri içerdiğinden, YZ okuryazarlığının ayrılmaz bir parçası olarak değerlendirilebilir (D'Ignazio, 2017).

Bu bağlamda, Long ve Magerko (2020), YZ okuryazarlığını şu şekilde tanımlar: "Yapay zekâ okuryazarlığı, bireylerin YZ teknolojilerini eleştirel biçimde değerlendirebilmesini, YZ ile etkili şekilde iletişim kurmasını ve YZ'yı günlük yaşamda, çevrimiçi ortamda ve işyerinde bir araç olarak kullanabilmesini sağlayan bir yetkinlikler bütünüdür."

5. Veri Okuryazarlığı ile Yapay Zekâ Arasındaki İlişki

Dijital çağda bilgi üretimi, yönetimi ve değerlendirilmesi,

geleneksel bilgi okuryazarlığı sınırlarını aşan çok boyutlu yeterlikleri gerektirmektedir. Özellikle yapay zekâ (YZ) ve büyük veri teknolojilerinin bilgi sistemlerinde giderek yaygınlaşması, bireylerin hem veriyle hem de algoritmik süreçlerle anlamlı ve eleştirel bir ilişki kurmalarını zorunlu kılmaktadır. Bu bağlamda, veri okuryazarlığı ve YZ okuryazarlığı, bilgi bilimi disiplini içinde yeniden tanımlanan temel beceri alanları olarak öne çıkmaktadır. Veri okuryazarlığı, bireyin veriyi tanıma, toplama, değerlendirme, analiz etme ve paylaşma gibi süreçlerde yetkin olması anlamına gelir (Carlson vd., 2011). Bilgi bilimi açısından bu kavram; yalnızca teknik beceriler değil, aynı zamanda etik duyarlılık, bağlamsal değerlendirme ve eleştirel analiz yetkinliklerini de içermektedir (Calzada-Prado ve Marzal, 2013). Bu kapsamda, veri okuryazarlığı hem kullanıcıların bilgi sistemleriyle olan etkileşimini kolaylaştırmakta hem de kurumların bilgi hizmetlerinin kalitesini artırmaktadır. Ayrıca Dünya Sağlık Örgütü gibi kurumların “Data Literacy Charter”ı, bu yetkinliği herkes için erişilebilir, disiplinlerarası, etik ve süreç odaklı bir beceri olarak tanımlamıştır (Ebeling vd., 2021).

Öte yandan, YZ okuryazarlığı, bireylerin yapay zekâ sistemlerinin temel işleyişini anlamasını, çıktıları değerlendirmesini, bu sistemlerle etkileşime girmesini ve sosyal etkilerini sorgulamasını sağlayan bir yetkinlikler bütünüdür (Long ve Magerko, 2020). Bununla birlikte Yim (2024) tarafından gerçekleştirilen sistematik tarama, bu çerçeveye “enformasyon, veri, hesaplamalı okuryazarlık ve etik konular” bileşenlerini de dâhil etmiş ve YZ okuryazarlığının disiplinler arası yapısını vurgulamıştır. YZ sistemleri sıklıkla “kara kutu” yapılarla çalıştığından, bireylerin bu sistemleri yalnızca kullanmakla kalmayıp, eleştirel ve bilinçli bir kullanıcı olarak değerlendirebilmeleri önem taşımaktadır (Pasquale, 2015). YZ okuryazarlığı diğer okuryazarlık türleri ile farklı ilişkilere sahiptir (Tablo 2).

Veri okuryazarlığı, YZ sistemlerinin altyapısını oluşturduğundan YZ okuryazarlığının doğal bir parçasıdır. Makine öğrenimi sistemleri, veriler üzerinden öğrenir; bu nedenle model çıktılarının anlaşılabilmesi için kullanıcıların temel istatistik bilgisine sahip olmaları gerekir (Lintner, 2024). Bu iki okuryazarlık biçiminin birbirinin tamamlayıcısı olduğunu söyleyebiliriz. Çünkü çağdaş YZ uygulamaları büyük ölçüde veriyle eğitilmekte ve veriye dayalı çıkarımlar üretmektedir. Yani YZ

okuryazarlığına sahip bir bireyin, aynı zamanda temel veri okuryazarlığına da hâkim olması beklenir. Bu durumu, “YZ’nın güvenilirliğinin inşasında, veri okuryazarlığı YZ okuryazarlığının önkoşulu hâline gelmektedir” şeklinde ifade etmektedir. Ayrıca Data Literacy Charter’de (Veri Okuryazarlığı Bildirgesi), YZ araçlarının kullanılabilmesi için veri okuryazarlığı dâhil, uygulama, teknik-metodolojik ve sosyo-kültürel perspektiflerle yeterlikler geliştirme ihtiyacını belirtir (Stifterverband, 2021).

Bilgi bilimi perspektifinden bakıldığında, bu iki okuryazarlık türünün birleşimi, kullanıcıların yalnızca bilgiye erişmesini değil; aynı zamanda bilgi sistemlerinin algoritmik yapısını anlamasını, dijital önyargıları sorgulamasını ve şeffaflığı talep etmesini mümkün kılar. Akademik kütüphanelerde bilgi uzmanlarının metin madenciliği ve YZ destekli kataloglama gibi yapay zekâ araçlarıyla çalışmaları, bu profesyonellerin veri ve YZ okuryazarlığı konularında yetkinlik geliştirerek kullanıcılara rehberlik etme kapasitesini artırmalarının gerektiğini ortaya koymaktadır (Lo, 2024). Kütüphaneler, akademik bilgi hizmetleri ve dijital arşiv sistemleri, bu yetkinliklerin kazandırılacağı doğal öğrenme ortamlarıdır. Bilgi profesyonelleri, bu bağlamda kullanıcıların hem veri hem de YZ ile bilinçli etkileşim kurmasını sağlayacak rehberlik rolünü üstlenmektedir.

Bilgi bilimi perspektifinden bakıldığında, veri ve yapay zekâ okuryazarlığı iki ayrı kavram gibi görünse de, pratikte iç içe geçen ve birbirini tamamlayan yetkinlik setleri olarak değerlendirilebilir. Veri okuryazarlığı, YZ sistemlerinin temeli iken; YZ okuryazarlığı, bu sistemlerin anlamlandırılmasını, eleştirilmesini ve etik olarak kullanılmasını sağlar. Bu kesişim, hem bireylerde hem kurumlarda eğitim programları, bilgi sistemleri ve hizmet modellerinin yeniden tasarlanması için kritik bir zemin oluşturmaktadır.

6. Sonuç

Dijital çağın hızla evrilen bilgi ortamı, bireylerin yalnızca bilgiye erişim becerilerini değil, aynı zamanda bu bilgiyi oluşturan, şekillendiren ve işleyen teknolojileri de anlayabilme yetkinliğini zorunlu kılmaktadır. Bu bağlamda veri okuryazarlığı ve yapay zekâ okuryazarlığı, çağdaş bireyin eleştirel düşünme, dijital farkındalık ve etik değerlendirme kapasitesini güçlendiren iki temel bileşen olarak öne çıkmaktadır.

Tablo 2. Yapay zekâ okuryazarlığı ile diğer okuryazarlıkların ilişkisi

Okuryazarlık Türü	Tanım	Yapay Zekâ Okuryazarlığıyla İlişkisi
Dijital Okuryazarlık	Bilgisayarları ve dijital araçları kullanma becerisi	Bir önkoşul; yapay zekâyı anlamak için temel gerekliliktir.
Hesaplama Okuryazarlığı	Kod yazma ve programlama becerisi	Gerekli olmayabilir; geliştiriciler için önemli, kullanıcılar için değildir.
Bilimsel Okuryazarlık	Bilimin doğasını ve sınırlarını anlama	Makine öğrenimi süreçlerini anlamada yardımcı olabilir.
Veri Okuryazarlığı	Veriyi okuma, analiz etme ve tartışma becerisi	Makine öğrenimiyle örtüşür, yapay zekâ süreçlerini destekler.

Bu derleme çalışması, özellikle bilgi bilimi perspektifinden hareketle, bu iki okuryazarlık türü arasındaki teorik ve uygulamalı bağları ortaya koyarak, dijitalleşen toplumda bireylerin ve kurumların hangi yetkinliklerle donatılması gerektiğine dair bütüncül bir değerlendirme sunmuştur.

Veri okuryazarlığı, bilginin güvenilirliğini sorgulama, veriye dayalı karar alma ve veri etiği gibi kavramları içerirken; yapay zekâ okuryazarlığı, algoritmaların nasıl çalıştığını anlama, otomatik sistemlerle iş birliği yapma ve algoritmik kararların olası önyargılarını sorgulama gibi becerilerle daha karmaşık bir katmanı temsil etmektedir. Bu beceriler, bilgi sistemlerinin daha etkili kullanılmasını ve kurumların hizmet kalitesinin artırılmasını mümkün kılar. Çalışmada ele alınan literatür, bu iki okuryazarlığın bir rekabet içinde değil, tamamlayıcı bir ilişki içerisinde geliştiğini göstermektedir. Özellikle makine öğrenimi, büyük veri analitiği ve insan-makine etkileşimi gibi alanlar, bu yetkinliklerin birlikte ele alınmasını gerektirmektedir.

Eğitim sisteminden kütüphanelere, dijital platformlardan kamu politikalarına kadar geniş bir yelpazede veri ve yapay zekâ okuryazarlığına dair ihtiyaçlar artmaktadır. Bu bağlamda hem teknik becerilerin kazandırılması hem de eleştirel ve etik boyutların geliştirilmesi önem arz etmektedir. Bu çalışmada ortaya konan karşılaştırmalı analizler, vaka örnekleri ve literatür taramaları, söz konusu okuryazarlıkların yalnızca bireysel değil, aynı zamanda toplumsal düzeyde dijital eşitsizliklerin giderilmesi açısından da stratejik bir önem taşıdığını ortaya koymuştur.

Bilgi bilimi perspektifinden bakıldığında, veri ve YZ okuryazarlığı, bireylerin yalnızca bilgiye erişimini değil, aynı zamanda bilgi sistemlerinin algoritmik yapısını anlamasını, dijital önyargıları sorgulamasını ve şeffaflığı talep etmesini mümkün kılar. Akademik kütüphaneler, dijital arşiv sistemleri ve diğer bilgi hizmetleri, bu yetkinliklerin kazandırılmasında doğal öğrenme ortamları olarak kritik bir rol oynar. Bilgi profesyonelleri, kullanıcıların veri ve YZ ile bilinçli bir şekilde etkileşim kurmasını desteklemek için eğitim programları, atölyeler ve rehber kaynaklar geliştirerek bu dönüşümde öncü bir konuma sahiptir (Digital Promise, 2024).

Gelecekte, veri ve YZ okuryazarlığının yaygınlaşması için disiplinler arası iş birliği ve eğitim reformları kritik önem taşıyacaktır. Eğitim kurumları, K-12 müfredatlarından yükseköğretime kadar bu yetkinlikleri entegre etmeli, teknoloji şirketleri ise teknik olmayan kitlelere yönelik erişilebilir eğitim girişimleri sunmalıdır (Google, 2024; Microsoft, 2024). Ayrıca, YZ sistemlerinin şeffaflığını ve hesap verebilirliğini artırmak için politika yapıcılar, etik standartlar ve düzenlemeler geliştirmelidir. Büyük dil modelleri gibi yeni nesil YZ teknolojilerinin yükselişi, bu yetkinliklerin sürekli öğrenme ve uyarılma gerektirdiğini göstermektedir (DataCamp, 2025).

Sonuç olarak, dijital çağın karmaşıklığı karşısında bireylerin sadece veriyle çalışabilen değil, aynı zamanda veriyi ve yapay zekâyı anlamlandırabilen, sorgulayabilen

ve etik ilkeler doğrultusunda kullanabilen bireyler olması gerekmektedir. Veri ve YZ okuryazarlığı, dijital çağın bilgi yoğun ekosisteminde bireyleri güçlendiren, eleştirel düşünme ve etik farkındalığı teşvik eden temel yetkinliklerdir. Bu beceriler, bireylerin bilgi sistemleriyle daha bilinçli ve etkili bir şekilde etkileşim kurmasını sağlarken, kurumların ve toplumun dijital dönüşümden maksimum fayda sağlamasına olanak tanır. Bilgi bilimi, bu yetkinliklerin geliştirilmesinde lider bir rol üstlenerek, dijital çağın eleştirel yetkinliklerini şekillendirmeye devam edecektir. Bu bağlamda, eğitimciler, bilgi uzmanları, politika yapıcılar ve teknoloji geliştiriciler için veri ve yapay zekâ okuryazarlığını bütüncül bir biçimde ele alan stratejilere ihtiyaç duyulmaktadır. Geleceğin bilgi toplumu, ancak bu tür eleştirel ve çok katmanlı dijital yetkinliklerle inşa edilebilir.

Katkı Oranı Beyanı

Yazarın katkı yüzdeleri aşağıda verilmiştir. Yazar makaleyi incelemiş ve onaylamıştır.

%	E.D.
K	100
T	100
Y	100
VTI	100
VAY	100
KT	100
YZ	100
GR	100
PY	100

K= kavram, T= tasarım, Y= yönetim, VTI= veri toplama ve/veya işleme, VAY= veri analizi ve/veya yorumlama, KT= kaynak tarama, YZ= Yazım, GR= gönderim ve revizyon, PY= proje yönetimi.

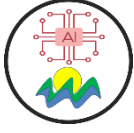
Çatışma Beyanı

Yazar bu çalışmada hiçbir çıkar ilişkisi olmadığını beyan etmektedirler.

Kaynaklar

- Almatrafi, O., Johri, A., & Lee, H. (2024). A systematic review of AI literacy conceptualization, constructs, and implementation and assessment efforts (2019–2023). *Computers and Education Open*, 6, 100173. <https://doi.org/10.1016/j.caeo.2024.100173>
- Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.
- Calzada Prado, J., & Marzal, M. Á. (2013). Incorporating data literacy into information literacy programs: Core competencies and contents. *Libri*, 63(2), 123–134. <https://doi.org/10.1515/libri-2013-0009>
- Carlson, J., Fosmire, M., Miller, C., & Nelson, M. S. (2011). Determining data information literacy needs: A study of students and research faculty. *portal: Libraries and the Academy*, 11(2), 629–657. <https://doi.org/10.1353/pla.2011.0022>
- DataCamp. (2025). *The state of data & AI literacy report 2025*. <https://www.datacamp.com/blog/introducing-the-state-of-data-and-ai-literacy-report-2025>

- Dhar, V. (2013). Data science and prediction. *Communications of the ACM*, 56(12), 64–73. <https://doi.org/10.1145/2500499>
- D'Ignazio, C. (2017). Creative data literacy: Bridging the gap between the data-haves and data-have nots. *Information Design Journal*, 23(1), 6–18. <https://doi.org/10.1075/idj.23.1.03dig>
- Digital Promise. (2024, June 18). *AI literacy: A framework to understand, evaluate, and use emerging technology*. <https://digitalpromise.org/2024/06/18/ai-literacy-a-framework-to-understand-evaluate-and-use-emerging-technology/>
- Druga, S., Williams, R., Breazeal, C., & Resnick, M. (2017). "Hey Google is it ok if I eat you?" Initial explorations in child-agent interaction. In *Proceedings of the 2017 Conference on Interaction Design and Children* (pp. 595–600). ACM. <https://doi.org/10.1145/3078072.3079753>
- Ebeling, J., Koch, H., & Roth-Grigori, A. (2021). *Data literacy education an deutschen Hochschulen: Kompetenzen im kritischen Umgang mit Daten*. Stifterverband.
- Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K., & Sandvig, C. (2015). "I always assumed that I wasn't really that close to [her]" Reasoning about invisible algorithms in news feeds. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 153–162). ACM. <https://doi.org/10.1145/2702123.2702154>
- Eslami, M., Vaccaro, K., Lee, M. K., Elazari Bar On, A., Gilbert, E., & Karahalios, K. (2019). User attitudes towards algorithmic opacity and transparency in online reviewing platforms. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). ACM. <https://doi.org/10.1145/3290605.3300835>
- Fast, E., & Horvitz, E. (2017). Long-term trends in the public perception of artificial intelligence. *Proceedings of the AAAI Conference on Artificial Intelligence*, 31(1). <https://doi.org/10.1609/aaai.v31i1.10635>
- Google. (2024). *Advancing education using Google AI*. Google for Education. https://edu.google.com/intl/ALL_us/ai/education/
- Gu, X., & Ericson, B. J. (2025). *AI literacy in K-12 and higher education in the wake of generative AI: An integrative review* (arXiv:2503.00079). arXiv. <https://doi.org/10.48550/arXiv.2503.00079>
- Gunning, D. (2017). *Explainable artificial intelligence (XAI)*. Defense Advanced Research Projects Agency (DARPA).
- Kahn, K., & Winters, N. (2017). Child-friendly programming interfaces to AI cloud services. In *Proceedings of the 12th European Conference on Technology Enhanced Learning (ECTEL 2017)* (pp. 566–570). Springer. https://doi.org/10.1007/978-3-319-66610-5_52
- Lintner, T. (2024). A systematic review of AI literacy scales. *npj Science of Learning*, 9(1), 50. <https://doi.org/10.1038/s41539-024-00262-1>
- Lo, L. S. (2024). Evaluating AI literacy in academic libraries: A survey study with a focus on US employees. *College & Research Libraries*, 85(5), 635. <https://doi.org/10.5860/crl.85.5.635>
- Long, D., & Magerko, B. (2020). What is AI literacy? Competencies and design considerations. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–16). ACM. <https://doi.org/10.1145/3313831.3376727>
- Microsoft. (2024). *AI in education: A Microsoft special report*. <https://www.microsoft.com/en-us/education/msdownloads/AI-in-Education-A-Microsoft-Special-Report.pdf>
- Mills, K., Ruiz, P., Lee, K. W., Coenraad, M., Fusco, J., Roschelle, J., & Weisgrau, J. (2024). *AI literacy: A framework to understand, evaluate, and use emerging technology*. Institute of Educational Sciences.
- Pangrazio, L., & Selwyn, N. (2021). Towards a school-based 'critical data education'. *Pedagogy, Culture & Society*, 29(3), 431–448. <https://doi.org/10.1080/14681366.2020.1739278>
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Pinski, M., & Benlian, A. (2024). AI literacy for users—A comprehensive review and future research directions of learning methods, components, and effects. *Computers in Human Behavior: Artificial Humans*, 2(1), 100062. <https://doi.org/10.1016/j.chbah.2024.100062>
- Shapiro, R. B., Fiebrink, R., & Norvig, P. (2018). How machine learning impacts the undergraduate computing curriculum. *Communications of the ACM*, 61(11), 27–29. <https://doi.org/10.1145/3274241>
- Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., Hirschberg, J., Kalyanakrishnan, S., Kamar, E., & Kraus, S. (2022). *Artificial intelligence and life in 2030: The one hundred year study on artificial intelligence* (arXiv:2211.06318). arXiv. <https://doi.org/10.48550/arXiv.2211.06318>
- Touretzky, D., Gardner-McCune, C., Martin, F., & Seehorn, D. (2019). Envisioning AI for K-12: What should every child know about AI? *Proceedings of the AAAI Conference on Artificial Intelligence*, 33(1), 9795–9799. <https://doi.org/10.1609/aaai.v33i01.33019652>
- Yim, I. H. Y. (2024). A critical review of teaching and learning artificial intelligence (AI) literacy: Developing an intelligence-based AI literacy framework for primary school education. *Computers and Education: Artificial Intelligence*, 7, 100319. <https://doi.org/10.1016/j.caeai.2024.100319>
- Zimmerman, M. (2018). *Teaching AI: Exploring new frontiers for learning*. International Society for Technology in Education.



YAPAY ZEKA ÇAĞINDA BİLGİSAYAR AĞLARI YÖNETİMİ VE GÜVENLİĞİ

Serkan VARAN^{1*}

¹Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye

Özet: Veri miktarının artmasına bağlı olarak, yapay zekanın bilgisayar ağlarıyla olan etkileşimi çok sayıda yeniliğe yol açtı. Ağlar üzerinde büyük miktarda veri akışı, toplumu ileriye taşıyan bir yenilik olarak karşımıza çıktı. Modern toplumda bilgi iletimi ve işlenmesi için önemli bir yöntem olan bilgisayar ağ teknolojisi, muazzam dönüşümler geçirmektedir. Büyük veri kavramı, ağ mimarisi, protokoller ve hatta güvenlik önlemleri için benzeri görülmemiş zorluklar ve fırsatları beraberinde getirmektedir. Aynı zamanda, yapay zeka teknolojilerinin hızla ilerlemesi bu olguyu daha da güçlendirmektedir. Ağ güvenliğinin ve yönetiminin her aşaması, yapay zekanın sunduğu verimliliği ve akıllı çözümleri kullanmaya başlamıştır. Bu sinerji, ağ teknolojisini geleneksel sınırların ötesine taşımakta ve daha fazla zeka ve verimlilik vaat eden bir geleceğe doğru ilerlemektedir.

Anahtar kelimeler: Büyük veri, Yapay zeka, Ağ güvenliği, Ağ yönetimi

Computer Network Management and Security in the Age of Artificial Intelligence

Abstract: Due to the increasing amount of data, the interaction of artificial intelligence with computer networks has led to many innovations. The flow of large amounts of data over networks has emerged as an innovation that moves society forward. Computer network technology, an important method for transmitting and processing information in modern society, is undergoing tremendous transformations. The concept of big data brings with it unprecedented challenges and opportunities for network architecture, protocols, and even security measures. At the same time, the rapid advancement of artificial intelligence technologies further strengthens this phenomenon. Every stage of network security and management has begun to use the efficiency and intelligent solutions offered by artificial intelligence. This synergy is taking network technology beyond traditional boundaries and moving towards a future that promises greater intelligence and efficiency.

Keywords: Big data, Artificial intelligence, Network security, Network management

*Sorumlu yazar (Corresponding author): Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye

E mail: svaran@omu.edu.tr (S. VARAN)

Serkan VARAN  <https://orcid.org/0000-0001-7669-9709>

Gönderi: 09 Mayıs 2025

Received: May 09, 2025

Kabul: 30 Mayıs 2025

Accepted: May 30, 2025

Yayınlanma: 15 Haziran 2025

Published: June 15, 2025

Cite as: Varan, S. (2025). Computer network management and security in the age of artificial intelligence. *Black Sea Journal of Artificial Intelligence*, 1(1), 31-34.

1. Giriş

Küresel veri hacimlerinde olağanüstü bir artışla işaretlenen bir çağda, "büyük veri" terimi akademideki kökenlerini aşmış ve kamu bilincine nüfuz etmiş, tanımını yalnızca veri kümeleri koleksiyonunun ötesine taşıyarak teknoloji, sosyal dinamikler ve hatta politika yapımında bir direktifin karmaşık bir birleşimini somutlaştırmıştır. Benzer şekilde, "yapay zeka" bilim kurguya yerleşmiş bir kavramdan çağdaş teknolojilerin ilerlemesini ilerleten temel güç haline gelmiştir. Bu bağlamda, bu varlıklar arasındaki etkileşim artık tek yönlü değil, karmaşık ve etkileşimli bir ilişkiye dönüşmüştür (Nowroozi vd., 2025). Bilgisayar ağ teknolojisi tüm toplumsal katmanları kesiştiren bir yaşam kaynağı olarak hizmet ettiğinden, bu yoğun veri işleyişi ve evrimi, temel roller üstlenmek için yapay zekayı acilen kullanmak zorundadır. Ağ teknolojileri ve toplumsal yaşam arasındaki bu entegrasyon, verimliliği

artırmak, güvenliği güçlendirmek ve sunulan sayısız zorlukla yüzleşmek için zorunludur. Bu yeni paradigmaya göre, yapay zekanın bilgisayar ağları alanında uygulanması hem teknik bir bilmece hem de iş ve günlük yaşamı kökten değiştirebilecek kritik bir belirleyici olarak karşımıza çıkmaktadır (Marino vd., 2025).

Bu çalışmanın amacı, büyük verinin karakteristik özelliklerini ortaya çıkararak, bilgisayar ağları yönetimi ve güvenliğinde kullanılan yapay zeka teknolojilerini açıklamaktır.

2. Büyük Verinin Karakteristik Özellikleri

Bilgi çağının gelmesiyle birlikte, bireyler giderek verinin toplumsal başkalaşımı ve 'Büyük Veri' çağının gelişyle başlayan teknolojik yeniliği ilerleten yeni bir motor olarak ortaya çıktığını fark ettiler. Büyük Veri çağı, internet, Nesnelerin İnterneti ve genişleyen bir dizi akıllı cihaz aracılığıyla üretilen hacimli veri hazineleriyle



karakterize edilir, zorluklar yaratır ve geleneksel veri işleme metodolojileri üzerinde güçlü etkiler uygularken, aynı zamanda sayısız endüstriye dönüştürücü gelişmeler olasılığı sunar (Altunay, 2024). Bu çağın bağlamında, veri hacimlerindeki büyüme en belirgin ayırt edici özellik olarak durmaktadır. Her saniye, sayısız birey ve makine muazzam miktarda veri üretmekte, sosyal medyanın metinlerinden, görüntülerinden ve videolarından ticari işlemlerin kayıtlarına, IoT cihazlarından gelen sensör okumalarına ve kapsamlı tıbbi görüntüleme veri kümelerine kadar bu veri çok çeşitli olarak karşımıza çıkmaktadır (Qiao, 2025). İçeride gizlenen bilgiler terabaytlardan (TB) petabaytlara (PB) ve hatta eksabaytlara (EB) sıçramıştır. Bu noktada bu verilerin yönetimi ve güvenliğinin sağlanması veri merkezleri ortaya çıkmıştır. Veri Merkezi, İnternet ağ altyapısında veri bilgilerini iletmek, hızlandırmak, görüntülemek, hesaplamak ve depolamak için kullanılan belirli ekipmanlardan oluşan küresel bir ağıdır. Veri merkezinin elektronik bileşenlerinin çoğu, düşük voltajlı DC güç kaynakları tarafından çalıştırılır. Veri türlerinin çeşitliliği de benzer şekilde gelişmekte olup, çeşitli biçimlerde ve karmaşık yapılarla sunulmaktadır. Veritabanı tabloları gibi geleneksel yapılandırılmış veriler artık tüm talepleri karşılamaya yetmemektedir; metin, resim ve video gibi yapılandırılmamış veri türleri ve e-postalar ile günlük dosyaları gibi yarı yapılandırılmış içerikler Büyük Veri'nin heterojenliğini oluşturmaktadır. Bireylerin davranışsal verileri ve makinelerin operasyonel verileri de dikkate alınmak üzere kapsamaktadır (Lacava vd., 2025). Hem veri hacmindeki hem de çeşitlilikteki artışla birlikte veri işleme hızlarına yönelik talep de artmaktadır. İşletmeler ve organizasyonlar, piyasa dalgalanmalarına yanıt olarak hızlı kararlar almak için bu geniş veri kümelerini gerçek zamanlı olarak analiz etmeyi arzulamaktadır ve bu da veri işleme teknolojilerine yönelik talepleri artırmaktadır. Örneğin, gerçek zamanlı veri işleme ve akış hesaplamasının gelişen alanı, bu hız arayışını ele almaya hizmet etmektedir. Belki de en heyecan verici değişim, verinin içsel değerinin yükselişinde ve kazılmasında yatmaktadır. Her veri kümesinin içinde keşfedilmeyi bekleyen gizli bir değer bulunmaktadır. Büyük verinin üç temel bileşeni olan hacim, hız ve çeşitlilik kavramları Şekil 1'de gösterilmiştir. İşletmeler ve araştırma kurumları, desenleri belirlemek, eğilimleri tahmin etmek ve devasa veri kümelerinden stratejiler geliştirmek için veri madenciliği, makine öğrenimi ve yapay zekanın güçlerinden yararlanmaktadır. Örneğin, e-ticaret platformları kullanıcı davranış verilerini analiz ederek daha kişiselleştirilmiş ürün önerileri sunabilir; doktorlar hasta sağlık kayıtlarının analizi yoluyla hastalıkları daha yüksek bir hassasiyetle teşhis edebilir. Yine de, bu umut vadeden yeni alan, pek çok zorluğu da barındırmaktadır. Veri güvenliği ve gizliliğin korunması yaygın olarak tartışılan endişeler haline gelmiştir. Bireysel gizliliği korurken verilerin değerini nasıl çıkaracağımız ve veri kullanımının sunduğu kolaylıklardan yararlanırken bilgi

ihlallerini nasıl önleyeceğimizle ilgili sorular, sektör uzmanlarının, akademisyenlerin ve politika yapımcıların topluca ele alması gereken konulardır (Altunay, 2025).



Şekil 1. Büyük verinin temel bileşenleri.

3. Yapay Zeka Çağında Network Yönetimi ve Güvenliği

Siber güvenlik, ağ sistemlerini yetkisiz erişimden, saldırılardan ve diğer olası tehlikelerden korumak için teknolojik ve yönetsel stratejiler kullanan kapsamlı bir kavramdır. Temel ilkeleri yalnızca verilerin bütünlüğünü ve kullanılabilirliğini korumayı değil, aynı zamanda bilgilerin gizliliğini sağlamayı ve böylece hassas ayrıntıların ifşa edilmesini önlemeyi amaçlar. Sürekli gelişen ve evrimleşen bu dijital alemde, yapay zeka siber güvenlik alanında vazgeçilmez bir güç olarak ortaya çıkmıştır. Siber güvenlik alanında titiz ve hassas bir bekçi olarak, yapay zeka teknolojileri, güvenlik tehditlerinin ve savunma önlemlerinin artan karmaşıklığına otomatik olarak uyum sağlamak ve uyum sağlamak için makine öğrenimi algoritmalarını uygular. Veri yığınlarının ortasında, yapay zeka yorulmak bilmeden günlük dosyalarını analiz eder, anormal davranışları izler ve hatta tehditlerdeki eğilimleri tahmin eder. Geleneksel güvenlik yöntemleriyle yan yana getirildiğinde, yapay zeka yeni ortaya çıkan kötü amaçlı yazılımları ve sıfırcı gün güvenlik açıklarını daha hızlı bir şekilde belirleyebilir ve bunlara yanıt verebilir (Altunay ve Albayrak, 2024). İnternet etkileşimlerinin hareketlerinde, sayısız güvenlik tuzağı gizlidir. Bilgisayar korsanları taktiklerini sürekli olarak geliştirirken, yapay zeka bu zorlukların üstesinden gelmek için devamlı eğitilir. Örneğin, yapay zeka, derin öğrenme becerisi sayesinde, çok sayıda kimlik avı e-postasındaki ince kalıpları ayırt edebilir, böylece bunları filtreleyebilir ve kullanıcıları aldatmadan koruyabilir. Özellikle evrimleşen sinir ağları, uzun kısa süreli bellek ve otokodlayıcılar bu alanda kullanılmaktadır. Akıllı sistemler, kendilerini durmaksızın geliştirmek için mevcut bilgilerini kullanır ve böylece giderek daha da aşılmaz bir dijital kale inşa eder. Dahası, yapay zekanın siber güvenlik çözümlerine entegre edilmesi daha karmaşık erişim kontrolüne olanak tanır. Akıllı teknoloji, kullanıcı davranış kalıplarını inceleyerek olası iç

tehditlere daha hızlı tepki verebilir. Belirli kullanıcıların tipik faaliyetlerini tanır ve kullanıcı kimlik bilgilerinin kötüye kullanılması gibi anormal faaliyetleri tespit ettiğinde derhal uyarılar yayınlar ve hassas verilere ve kritik altyapıya uygunsuz erişimi kısıtlar. Somut dünyada, finans kuruluşlarının siber güvenlik uygulamaları öğretici bir örnek sunar. Son yıllarda, birkaç banka finansal dolandırıcılıkla mücadele etmek için yapay zeka destekli güvenlik sistemleri konuşlandırmaya başladı. Sürekli olarak çeşitli işlem verilerinden öğrenen bu sistemler, bir müşterinin olağan modelinden sapan işlemleri anında belirleyebilir ve potansiyel dolandırıcılık eylemlerini derhal önleyebilir, böylece müşterilerin finansal varlıklarını koruyabilir (Lin, 2024).

İnternetin geniş evreninde, ağ yönetimi ve optimizasyonu, hızlı ve verimli bilgi akışını sağlayarak akıllı bir gezgin gibi işlev görür. Bu sistemler, ağ koşullarının dikkatli bir şekilde izlenmesi, veri trafiğinin incelenmesi ve kaynak dağıtımının ayarlanması yoluyla ağ istikrarını ve en yüksek performansı sürekli olarak korur. Yapay zekanın hızlı evrimiyle, ağ yönetimi ve optimizasyonunun tüm yönlerine sızmıştır. Derin öğrenme gibi teknolojileri kullanan yapay zeka tabanlı sistemler, kafa karıştırıcı bir senfonideki melodiyi ayırt etmeye benzer şekilde, ağ verilerinin karmaşıklıkları arasında trafik modellerini ayırt edebilir. Sadece en yüksek kullanım sürelerini tahmin etmekle kalmaz, aynı zamanda olası tehlikeleri önlemek için önceden alarm sinyali veren dikkatli koruyucular olarak hareket ederek anormal trafiği hızla belirlerler. Yapay zeka, ağ kaynak tahsisinde kayda değer ilerlemeler kaydetmiştir. Bant genişliği kullanımını gerçek zamanlı olarak optimize etti ve kaynakların gerektiği gibi kullanıcılar arasında dağıtılmasını sağlamak için veri yönlendirmesini hassasiyetle yürüttü (Yao vd., 2025). Böylece, her veri paketi en verimli rota boyunca yönlendirilir, bu da geniş dijital alemde özel bir yol oluşturmaya benzer. Örneğin, yapay zeka görüntülü konferans talebinde bir artış tespit ettiğinde, derhal ek bant genişliği tahsis eder, kesintisiz iletişimi kolaylaştırmak ve önemli toplantıların sorunsuz bir şekilde yürütülmesini sağlamak için geniş bir bilgi köprüsü oluşturur. Dahası, yapay zeka sürekli öğrenme ve kendini iyileştirmede mükemmeldir, böylece ağ yönetiminin zekasını geliştirir. Yeterli bir geçmiş veri kümesi topladıktan sonra, yapay zeka gelecekteki ağ ihtiyaçlarını daha doğru bir şekilde tahmin edebilir, dalgalanan yükleri karşılamak ve kaynak israfını önlemek için ağ stratejilerini dinamik olarak ayarlayabilir. Böyle bir ağ yönetim sistemi, deneyimli bir stratejistin ağ kaynaklarının verimli kullanımını en üst düzeye çıkarması gibi, sürekli öğrenme, tahmin ve ayarlama yoluyla bilgeliliğini keskinleştirir. Bununla birlikte, teknolojik gelişmeler asla izole bir şekilde gerçekleşmez. Ağ optimizasyonunun sağlanmasında da yapay zeka araçları önemli bir yer tutar. Herhangi bir donanım eklemekten gelişmiş araçlar ve özelleştirilmiş ağ yapılandırılmaları sayesinde ağ verimliliği

arttırılabilmektedir. Yapay zeka ağ optimizasyonunu iyileştirdikçe, gizlilik ve güvenlik hususları en önemli hale gelir. Her ilerleme, veri hassasiyeti ve olası ağ güvenlik açıklarının derinlemesine anlaşılması ve dikkatli bir şekilde değerlendirilmesine dayanmalıdır. Bu nedenle, teknolojinin uygulanmasına devam eden keşif ve olası etik ve güvenlik sorunlarının derinlemesine düşünülmesi eşlik eder ve akıllı optimizasyonun gelecekteki ağ ortamının istikrarı ve güvenliğiyle el ele ilerlemesini sağlar (Effah vd., 2025). Günümüzde pek çok yapay zeka tabanlı araç bilgisayar ağlarının yönetiminde ve güvenliğinin sağlanmasında kullanılmaktadır. Bu araçlar Tablo 1’de gösterilmiştir.

Tablo 1. Bilgisayar ağlarının yönetiminde ve güvenliğinde kullanılan yapay zeka tabanlı araçlar

Araç Adı	Alan
IBM /Watson (Newman, 2018)	Yönetim ve güvenlik
Juniper Networks (Madrid, 2020)	Yönetim ve güvenlik
Balbix Breach Control (Bablix, 2021)	Güvenlik
bioHAIFCS (Demertzis ve Iliadis, 2015)	Güvenlik
CyberSecTK (Calix vd., 2020)	Güvenlik
Vectra Cognito (Vectra, 2021)	Yönetim ve güvenlik
DefPloreX (Balduzzi ve Maggi, 2017)	Yönetim ve güvenlik
IBMQRadar (IBM, 2021)	Güvenlik
StringSifter (Stigsifter, 2020)	Yönetim ve güvenlik
InterceptX (Intercept, 2020)	Güvenlik
TAA (Symantech, 2018)	Yönetim ve güvenlik

4. Tartışma ve Sonuç

Büyük veri ve yapay zeka arasındaki sinerjik etkileşim, bilgisayar ağ teknolojisinin ilerlemesi için sınırsız umutlar müjdelemektedir. Ağ güvenliği, yönetimi, veri analitiği ve hatta bulut bilişim alanlarındaki uygulamalarına derinlemesine inerek, yapay zeka hızla bilgisayar ağlarının entelektüelleştirilmesi için vazgeçilmez bir katalizör haline gelmektedir. Bununla birlikte, verilerin gizliliğini ve güvenliğini korumak, yapay zeka sistemlerinin şeffaflığını ve yorumlanabilirliğini artırmak ve insan uzmanlığıyla en uygun iş birliğini belirlemek de dahil olmak üzere bir dizi zorlukla karşı karşıya kalınması gerekmektedir. İleriye bakıldığında, teknolojik yenilikler bu alanlardaki bilgisayar ağlarının olgunlaşmasını ilerletmeye devam edecek ve yapay zekanın geniş veri depolarıyla entegrasyonuna daha fazla vurgu yaparak, böylece bir bütün olarak toplumsal ilerlemeyi hızlandıracaktır.

Katkı Oranı Beyanı

Yazarın katkı yüzdeleri aşağıda verilmiştir. Yazar makaleyi incelemiş ve onaylamıştır.

%	N.K.
K	100
T	100
Y	100
VTI	100
VAY	100
KT	100
YZ	100
GR	100
PY	100

K= kavram, T= tasarım, Y= yönetim, VTI= veri toplama ve/veya işleme, VAY= veri analizi ve/veya yorumlama, KT= kaynak tarama, YZ= Yazım, GR= gönderim ve revizyon, PY= proje yönetimi.

Çatışma Beyanı

Yazar bu çalışmada hiçbir çıkar ilişkisi olmadığını beyan etmektedirler.

Kaynaklar

- Altunay, H. C. (2024). Analysis of cyber attacks using honeypot. *Black Sea Journal of Engineering and Science*, 7(5), 954–959. <https://doi.org/10.52704/bssscience.1481075>
- Altunay, H. C. (2025, April 24–25). *Dijital ekonomi ve blok zinciri uygulamaları* [Bildiri sunumu]. 5. Uluslararası Yapay Zeka ve Veri Bilimi Kongresi, İzmir, Türkiye.
- Altunay, H. C., & Albayrak, Z. (2024). SMS spam detection system based on deep learning architectures for Turkish and English messages. *Applied Sciences*, 14(24), 11804. <https://doi.org/10.3390/app142411804>
- Balbix. (2021). *Balbix BreachControl*. <https://www.balbix.com/product-overview/>
- Balduzzi, M., & Maggi, F. (2017). *DefPloreX: A machine-learning toolkit for large-scale eCrime forensics*. Trend Micro. <https://blog.trendmicro.com/trendlabs-security-intelligence/defplorex-machine-learning-toolkit-large-scale-ecrime-forensics/>
- Calix, R. A., Singh, S. B., Chen, T., Zhang, D., & Tu, M. (2020). Cyber security tool kit (CyberSecTK): A Python library for machine learning and cyber security. *Information*, 11(2), 100. <https://doi.org/10.3390/info11020100>
- Demertzis, K., & Iliadis, L. (2015). A bio-inspired hybrid artificial intelligence framework for cyber security. In N. Daras & M. Rassias (Eds.), *Computation, cryptography, and network security* (pp. 161–193). Springer. https://doi.org/10.1007/978-3-319-18275-9_7
- Effah, E. Q., Osei, E. O., Jnr, M. D., & Tetteh, A. (2024). Hybrid

approach to classification of DDoS attacks on a computer network infrastructure. *Asian Journal of Research in Computer Science*, 17(4), 19–43. <https://doi.org/10.9734/ajrcos/2024/v17i4427>

FireEye. (2020). *StringSifter: A machine learning tool that ranks strings based on their relevance for malware analysis* [Computer software]. GitHub. <https://github.com/mandiant/stringstifter>

IBM. (2021). *QRadar Advisor with Watson*. <https://www.ibm.com/in-en/products/cognitive-security-analytics>

Lacava, A., Bonati, L., Mohamadi, N., Gangula, R., Kaltenberger, F., Johari, P., & Melodia, T. (2025). dApps: Enabling real-time AI-based Open RAN control. *Computer Networks*, 254, 111342. <https://doi.org/10.1016/j.comnet.2024.111342>

Lin, Y. (2024). Application and challenges of computer networks in distance education. *Computer Performance and Communication Systems*, 8(1), 17–24.

Madrid, S. (2020). *Juniper strengthens connected security portfolio with new risk-based access control capabilities and remote access VPN*. Juniper Networks. <https://blogs.juniper.net/en-us/security/juniper-strengthens-connected-security-portfolio-with-new-risk-based-access-control-capabilities-and-remote-access-vpn>

Marino, D. L., Wickramasinghe, C. S., Rieger, C., & Manic, M. (2025). Self-supervised and interpretable anomaly detection using network transformers. *IEEE Transactions on Industrial Informatics*, 21(5), 4252–4261. <https://doi.org/10.1109/TII.2024.3414920>

Newman, L. H. (2018). AI can help cybersecurity—If it can fight through the hype. *Wired*. <https://www.wired.com/story/ai-machine-learning-cybersecurity>

Nowroozi, E., Haider, I., Taheri, R., & Conti, M. (2025). Federated learning under attack: Exposing vulnerabilities through data poisoning attacks in computer networks. *IEEE Transactions on Network and Service Management*, 22(1), 822–831. <https://doi.org/10.1109/TNSM.2024.3444055>

Qiao, W. (2025). Comprehensive framework for collaborative decision-making in evaluating computer network security using interval neutrosophic information. *Neutrosophic Sets and Systems*, 76, 520–537.

Sophos. (2020). *Intercept X: Stop unknown threats*. <https://www.sophos.com/en-us/products/intercept-x>

Symantec. (2018). *Targeted attack analytics*. Broadcom. <https://docs.broadcom.com/doc/targeted-attack-analytics-en>

Vectra AI. (2021). *Cognito Platform: Network detection and response built on artificial intelligence*. <https://www.vectra.ai/products/cognito-platform>

Yao, K., Pan, F., Liang, H., Zhang, X., Li, L., Song, L., & Lu, W. (2025). Shifting d-band center: An overlooked factor in broadening electromagnetic wave absorption bandwidth. *Advanced Functional Materials*, 35(3), 2413639. <https://doi.org/10.1002/adfm.202413639>