Mühendislik Bilimleri ve Tasarım Dergisi
13(4), 1047-1060, 2025
e-ISSN: 1308-6693

Journal of Engineering Sciences and Design
DOI: 10.21923/jesd.1717599

Araştırma Makalesi

Research Article

# YAPAY ZEKA DESTEKLİ IOT GÜVENLİK İZLEME SİSTEMİ

**Kıyas KAYAALP[1*], Tuba YILMAZ[1], Mukaddes KARABIYIK[1]**

[1]Isparta Uygulamalı Bilimler Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Isparta, Türkiye

**Anahtar Kelimeler**

*DDoS Tespiti,*
*IoT Güvenliği,*
*Yapay Zeka Tabanlı Tespit,*
*Makine Öğrenmesi,*
*Gerçek Zamanlı İzleme.*

**Öz**

Bu çalışmada, IoT (Nesnelerin İnterneti) cihazlarının bağlı bulunduğu ağlarda gerçekleşen DDoS (Dağıtılmış Hizmet Engelleme) saldırılarının tespitine yönelik bir güvenlik sistemi geliştirilmiştir. IoT cihazlarının düşük işlem gücü, sınırlı bellek kapasitesi ve zayıf güvenlik önlemleri nedeniyle bu cihazlar, siber saldırganlar tarafından sıklıkla hedef alınmaktadır. Bu doğrultuda, IoT tabanlı ağlarda sıkça rastlanan DDoS saldırılarının etkilerini azaltmak amacıyla denetimli öğrenme yöntemleriyle çalışan bir tespit modeli tasarlanmıştır. Modelin eğitimi için farklı DDoS saldırı türlerini içeren ve DDoS trafiğiyle etiketli bir veri seti kullanılmıştır. Eğitim sürecinde veri seti eğitim ve test kümelerine ayrılmış, modelin başarımı doğruluk, kesinlik, hatırlama ve F1 skoru metrikleriyle değerlendirilmiştir. Ayrıca, k-fold çapraz doğrulama uygulanarak modelin genelleme yeteneği artırılmıştır. Sistem yalnızca statik veri ile sınırlı kalmamış, canlı ağ trafiğini de analiz edebilecek biçimde yapılandırılmıştır. Gerçek zamanlı olarak analiz edilen ağ trafiği üzerinden DDoS saldırıları başarıyla tespit edilmiş ve kullanıcıya anlık bildirimler sağlanmıştır. Böylece, IoT ağlarına yönelik saldırılara karşı etkin, dinamik ve yapay zeka tabanlı bir tespit mekanizması ortaya konulmuştur.

# ARTIFICIAL INTELLIGENCE-BASED IOT SECURITY MONITORING SYSTEM

**Keywords**

*DDoS Detection,*
*IoT Security,*
*AI-Based Detection,*
*Machine Learning,*
*Real-Time Monitoring.*

**Abstract**

In this study, a security system was developed to detect Distributed Denial of Service (DDoS) attacks targeting networks connected to Internet of Things (IoT) devices. Due to their low processing power, limited memory capacity, and inadequate security measures, IoT devices are frequently targeted by cyber attackers. Accordingly, a detection model based on supervised learning techniques was designed to mitigate the impact of DDoS attacks, which are commonly encountered in IoT-based networks. For model training, a labeled dataset containing various types of attacks and DDoS-related traffic was utilized. During the training process, the dataset was divided into training and testing subsets, and the model's performance was evaluated using accuracy, precision, recall, and F1-score metrics. In addition, k-fold cross-validation was applied to enhance the model's generalization ability. The system was structured not only to work with static data but also to analyze live network traffic. DDoS attacks were successfully detected through real-time traffic analysis, and instant alerts were delivered to the user. As a result, an effective, dynamic, and AI-based detection mechanism was established against attacks targeting IoT networks.

**Alıntı / Cite**

Kayaalp, K., Yılmaz, T., Karabıyık, M., (2025). Yapay Zeka Destekli IoT Güvenlik İzleme Sistemi, Mühendislik Bilimleri ve Tasarım Dergisi, 13(4), 1047-1060.

**Yazar Kimliği / Author ID (ORCID Number)**

K. Kayaalp, 0000-0002-6483-1124
T. Yılmaz, 0009-0000-5587-7895
M. Karabıyık, 0009-0002-5835-6651

| **Makale Süreci / Article Process** | |
|---|---|
| **Başvuru Tarihi / Submission Date** | 11.06.2025 |
| **Revizyon Tarihi / Revision Date** | 08.09.2025 |
| **Kabul Tarihi / Accepted Date** | 27.10.2025 |
| **Yayım Tarihi / Published Date** | 30.12.2025 |

[*] İlgili yazar / Corresponding author: kiyaskayaalp@isparta.edu.tr, +90-246-214-6792

# ARTIFICIAL INTELLIGENCE-BASED IOT SECURITY MONITORING SYSTEM

Kıyas KAYAALP[1*], Tuba YILMAZ[1], Mukaddes KARABIYIK[1]
[1]Isparta University of Applied Sciences, Faculty of Technology, Department of Computer Engineering, Isparta, Türkiye

**Highlights**

- A real-time DDoS detection system is developed for IoT networks.
- Machine learning algorithms are used to classify network traffic.
- Live traffic is analyzed alongside static datasets.
- AI-based architecture provides dynamic threat response.

**Purpose and Scope**

This study aims to develop an AI-powered security monitoring system for detecting DDoS attacks in IoT-based networks. The system addresses the increasing security threats posed by IoT devices due to their limited resources and weak protection mechanisms.

**Design/methodology/approach**

A labeled dataset containing various attack types and normal traffic was used to train a machine learning model. The model was evaluated using accuracy, precision, recall, and F1-score metrics, and k-fold cross-validation was applied to improve generalizability. In addition to static data, real-time traffic was monitored and analyzed.

**Findings**

The developed system successfully detected DDoS attacks in real-time network environments and promptly generated instant alerts to inform users about potential threats. The classification model exhibited high performance across multiple evaluation metrics, including accuracy, precision, recall, and F1-score, both during testing with labeled datasets and under live traffic conditions. These results indicate that the model is not only effective in controlled experimental settings but also robust and adaptable in dynamic, real-world scenarios. Furthermore, the system's ability to process both static and streaming data demonstrates its flexibility for integration into various IoT infrastructures. Overall, the findings confirm the model's capability to provide proactive, intelligent, and real-time defense mechanisms against DDoS attacks, thereby contributing to the enhancement of IoT network security.

**Research limitations/implications**

The model's performance may vary depending on the characteristics of the live network. Future studies may focus on expanding the dataset diversity and integrating adaptive learning mechanisms for evolving attack types.

**Practical implications**

The proposed system enhances the security of IoT networks by enabling proactive detection and prevention of DDoS attacks. It can be integrated into existing network infrastructures to improve resilience against cyber threats.

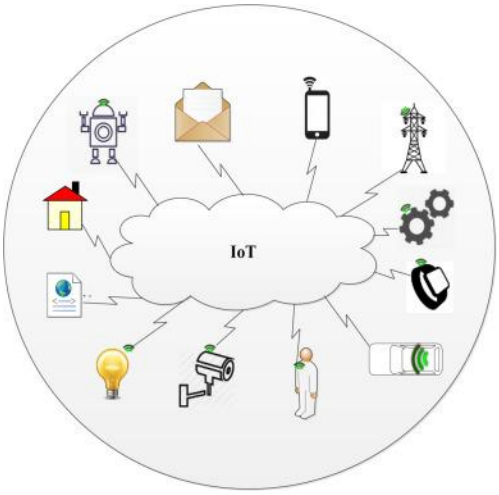
**Originality**

The originality lies in combining static dataset analysis with real-time traffic monitoring for DDoS detection in IoT networks. The system's applicability in resource-constrained environments adds practical and scientific value.

[*] Corresponding author: kiyaskayaalp@isparta.edu.tr, +90-246-214-6792

## 1. Giriş (Introduction)

İnternet, dünya genelinde milyarlarca cihazın birbirine bağlanmasını sağlayan, bilgi paylaşımını ve iletişimi mümkün kılan küresel bir ağ altyapısıdır (Kurtoğlu ve Süslü, 2024). Başlangıçta yalnızca bilgisayarlar arasında veri aktarımını amaçlayan bu yapı, zamanla gelişerek farklı cihazların da ağa dahil edilmesine olanak tanımıştır. Bu gelişimin bir sonucu olarak ortaya çıkan Nesnelerin İnterneti (IoT) kavramı Şekil 1'de görüldüğü üzere çeşitli fiziksel nesnelerin internet ağına entegre olarak birbirleriyle veri alışverişinde bulunmasını sağlayan bir teknoloji yaklaşımıdır.




**Şekil 1**. Nesnelerin interneti (Internet of things)

### 1.1. IoT Sistemlerinin Yapısı ve İşlevleri (The Structure and Functions of IoT Systems)

Günümüzde IoT sistemleri, yalnızca cihazları birbirine bağlamakla kalmayıp; sensörler, iletişim ağları, bilgi işlem altyapıları ve otomasyon yazılımlarını içeren bütüncül bir yapıyla çalışmaktadır. Bu sistemler, fiziksel nesnelerden veri toplayarak analiz etmekte, uzaktan kontrol imkânı sunmakta ve süreçleri optimize etmektedir. IoT teknolojileri sayesinde cihazlar çevrelerindeki diğer sistemlerle etkileşime geçmekte ve böylece ortak bir dijital ekosistem oluşturmaktadır. Bu yapı, bireysel kullanımdan endüstriyel uygulamalara kadar geniş bir yelpazede verimlilik artışı ve iş süreçlerinde kolaylık sağlamaktadır (Bıçakçı, 2019).

IoT teknolojisinin gelişimi, günlük yaşamı kolaylaştıran pek çok katkı sunarken, aynı zamanda bilgi güvenliği açısından önemli riskleri de beraberinde getirmektedir. Günümüzde "akıllı" olarak nitelendirilen telefonlar, televizyonlar, beyaz eşyalar, araçlar ve güvenlik sistemleri gibi cihazlar, aslında çeşitli güvenlik açıkları barındırmaktadır. Örneğin, 2013 yılında Rusya'nın Rossiya 24 televizyon kanalı, Çin'den ithal edilen bazı ütülerin kablosuz internet üzerinden casusluk yapabilecek çipler içerdiğini iddia etmiş; yapılan incelemelerle bu durum doğrulanmıştır. Ayrıca, bir evdeki tüm cihazların tek bir otomasyon sistemine bağlı olması, olası bir siber saldırı ile bu sistemin kontrol edilmesi yoluyla yangın çıkarma, hırsızlık gerçekleştirme veya kişisel verilere izinsiz erişim gibi tehditleri mümkün kılmaktadır. Bu durum, IoT cihazlarının güvenliğinin ne denli kritik olduğunu açıkça ortaya koymaktadır (Turak, 2015).

IoT ortamlarındaki temel güvenlik zorlukları; gizlilik, yetkilendirme, doğrulama, erişim kontrolü, sistem yapılandırması, bilgi depolama ve veri yönetimi gibi başlıklar altında toplanmaktadır. Gizlilik ihlalleri, cihazlar ile ağlar arasında iletilen verilerin kötü niyetli üçüncü tarafların eline geçmesiyle sonuçlanabilir. Yetkilendirme eksiklikleri, yalnızca yetkili kullanıcıların cihazlara erişimini sağlamakta yetersiz kalabilirken; doğrulama mekanizmalarındaki zayıflıklar, kimlik sahtekârlığı ve kötü niyetli cihaz kullanımını kolaylaştırmaktadır. Erişim kontrollerinin yetersiz olması, hassas verilere yetkisiz erişimi mümkün kılmaktadır. Ayrıca sistem yapılandırmasındaki yanlışlar, güvenlik açıklarını artırmakta; bilgi depolama ve yönetimindeki eksiklikler ise verilerin bütünlüğünü ve gizliliğini tehdit etmektedir. IoT cihazlarının sınırlı işlem kapasiteleri nedeniyle güçlü şifreleme tekniklerini kullanamaması da, bu sistemleri veri hırsızlığı ve ağ saldırılarına karşı savunmasız hâle getirmektedir. Tüm bu zorluklar, IoT teknolojisinin sunduğu avantajların siber tehditlerle gölgelenmemesi için etkin güvenlik çözümlerinin geliştirilmesini zorunlu kılmaktadır (Jing vd., 2014).

### 1.2. IoT ve Yapay Zeka Entegrasyonu (IoT and Artificial Intelligence Integration)

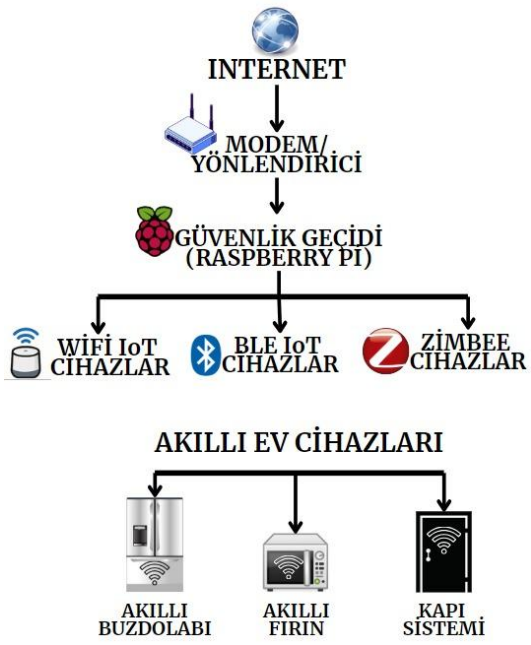
Nesnelerin İnterneti (IoT) araçlarının sayısı ve kullanım alanları her geçen gün artmaktadır. 2021 yılı itibarıyla

IoT cihaz sayısı %8'lik bir artışla 12.2 milyara ulaşmıştır. Bu hızlı artış, büyük miktarda veri üretimini beraberinde getirmekte ve bu verilerin işlenmesini ve yönetilmesini zorlaştırmaktadır. IoT ortamlarında ortaya çıkan hesaplama ve veri işleme ihtiyaçları, sistem performansı açısından kritik bir unsur hâline gelmiştir. Bu noktada, yapay zeka (AI) teknolojileri, IoT'nin güvenlik sorunlarının çözümünde ve diğer yeni teknolojilerle entegrasyonunda tamamlayıcı bir rol üstlenmektedir (Mohanta vd., 2020). Ghosh vd. (2018), yapay zekanın IoT'nin büyük ölçekli ve yapılandırılmamış verilerini işleme kapasitesi sayesinde, heterojen veri yapılarının gerçek zamanlı hesaplanmasını sağladığını ve sistemin işlevselliğini artırdığını belirtmiştir.

IoT sistemlerinin güvenlik ve veri işleme gereksinimlerini karşılamak adına öne çıkan bir diğer yaklaşım ise derin öğrenme algoritmalarıdır. Derin öğrenme, çok katmanlı yapay sinir ağları sayesinde büyük veri setlerindeki karmaşık ilişkileri öğrenebilmekte ve anlamlı desenler çıkarabilmektedir. IoT ortamlarında, bu algoritmalar büyüyen veri hacmini etkin biçimde analiz ederek sistem performansını optimize edebilmektedir. Özellikle yapılandırılmamış ve heterojen verilerin gerçek zamanlı işlenmesi, anormalliklerin tespiti ve olası tehditlere karşı önlem alınmasını mümkün kılmaktadır. Örneğin, ağ trafiğini analiz eden derin öğrenme tabanlı modeller, olağandışı aktiviteleri ve siber saldırıları erken aşamada tespit ederek sistem güvenliğini önemli ölçüde artırmaktadır. Ayrıca, kullanıcı davranışlarını öğrenerek yetkisiz erişimleri tespit etme ve engelleme yeteneğine sahiptir. Derin öğrenme algoritmaları, IoT cihazları arasındaki farklılıkları yönetmede etkili çözümler sunmakta ve cihazlar arası veri paylaşımını kolaylaştırmaktadır. Tüm bu özellikler, derin öğrenmeyi IoT sistemlerinde güvenlik ve veri yönetimi açısından vazgeçilmez bir teknoloji konumuna getirmektedir. Literatürde, yapay zekanın IoT güvenlik altyapılarına entegrasyonuna ilişkin çok sayıda çalışma yer almakta olup, bu çalışmalar AI tabanlı yaklaşımların anomali tespiti, veri analizi ve gerçek zamanlı tehdit izleme konularında kayda değer katkılar sağladığını göstermektedir. Böylece, IoT ağlarının karşı karşıya kaldığı karmaşık güvenlik sorunlarına karşı daha dinamik, esnek ve ölçeklenebilir çözümler geliştirilebilmektedir (Turak, 2015).

### 1.3. Çalışmanın Katkısı ve Önerilen Sistem (Contribution of the Study and Proposed System)

Bu çalışma kapsamında, IoT tabanlı ağlarda meydana gelen DDoS saldırılarını tespit edebilen, yapay zeka ve denetimli öğrenme temelli bir güvenlik sistemi geliştirilmiştir. Gerçekleştirilen sistemin çalışma yapısı Şekil 2'de verilmiştir. Sistem, hem etiketli veri kümeleriyle eğitilmiş bir model aracılığıyla yüksek doğruluk oranlarına ulaşmakta hem de gerçek zamanlı ağ trafiğini analiz ederek olası saldırılara karşı kullanıcıyı anlık olarak uyarmaktadır. Uygulamanın en dikkat çekici yönlerinden biri, düşük maliyetli ve düşük güç tüketimine sahip Raspberry Pi gibi donanımlarla entegre çalışabilecek şekilde tasarlanmış olmasıdır. Bu sayede, küçük ve orta ölçekli işletmeler veya bireysel kullanıcılar için erişilebilir, ekonomik ve uygulanabilir bir güvenlik çözümü sunulmaktadır. Geliştirilen sistem, IoT cihazlarının bulunduğu ağlarda erken tehdit tespiti sağlayarak güvenliği artırmayı ve ağ bütünlüğünün korunmasına katkıda bulunmayı hedeflemektedir.




**Şekil 2.** Proje şeması (Project diagram)

## 2. Kaynak Araştırması (Literature Survey)

Son yıllarda IoT tabanlı ağlarda güvenlik tehditlerinin artması, bu alanda çeşitli saldırı tespit yöntemlerinin geliştirilmesini zorunlu kılmıştır. Literatürde, farklı veri setlerine ve yöntemlere dayalı çok sayıda çalışma gerçekleştirilmiştir. Booij vd. (2021), ToN_IoT veri setinin analizini gerçekleştirerek; pcap dosyaları, Bro günlükleri, sensör verileri ve işletim sistemi loglarını birleştiren ilk IoT saldırı veri seti olduğunu belirtmiş, bu veri kümesinin yüksek düzeyde heterojen yapı sunduğunu ifade etmiştir. Söz konusu çalışma, farklı veri kümeleri arasında yapılan çapraz eğitimin performans düşüklüğüne yol açtığını ve standardizasyonun önemini vurgulamaktadır.

Mercan vd. (2025), IoT saldırılarını analiz etmek amacıyla çok sınıflı bir sınıflandırma sistemi geliştirmiş; bu sistemde büyük dil modellerinden (LLM) esinlenen bir yaklaşım kullanılmıştır. Yöntem, özellikle IoT-23 veri setindeki farklı saldırı tiplerini tespit edebilmek için tasarlanmıştır. LLM yaklaşımı, modelin çok sınıflı karar verme kabiliyetini güçlendirirken, sınıflandırma performansını artırmıştır. Elde edilen sonuçlar, sistemin farklı saldırı sınıflarını yüksek doğrulukla ayırabildiğini göstermektedir; bu da LLM bazlı çözümlerin IoT saldırı tespitinde umut verici bir yön olduğunu ortaya koymaktadır.

Ntayagabiri vd. (2025), IoT saldırılarının tespiti ve sınıflandırılması amacıyla farklı denetimli makine öğrenmesi algoritmalarını karşılaştırmalı olarak incelemiştir. Çalışmada birden fazla algoritma (ör. Random Forest, SVM, XGBoost) kullanılarak performans analizi yapılmış ve çeşitli IoT veri setleri üzerinde doğruluk, F1-skor ve hassasiyet gibi metriklerle değerlendirilmiştir. Sonuçlar, özellikle ağaç tabanlı yöntemlerin yüksek başarı sağladığını, ancak veri setine ve saldırı tipine göre performans farklılıkları görülebildiğini ortaya koymuştur. Bu çalışma, IoT saldırı tespitinde farklı denetimli algoritmaların güçlü ve zayıf yönlerini sistematik biçimde ortaya koyması açısından önemli bir katkı sunmaktadır.

Benzer biçimde, Woźniak vd. (2020), RNN-LSTM mimarisi ve NAdam optimizasyonu ile tehlikeli bağlantıların sınıflandırılmasını hedeflemiş, nanosaniyelik işlem süresiyle yüksek doğruluk oranı (%99.99) elde edilmiştir. Çalışma, gerçek zamanlı tehdit tespitinde düşük kaynak tüketimi açısından öne çıkmaktadır.

Derin öğrenme temelli çalışmalar da dikkat çekmektedir. Ullah ve Mahmoud (2021), CNN1D, CNN2D ve CNN3D modellerini kullanarak dört farklı IoT veri kümesini birleştirmiş ve %99'u aşan tespit oranları elde etmiştir. Sahu vd. (2021) ise 20 kötü amaçlı Raspberry Pi cihazından toplanan verilerle geliştirdikleri CNN modelinde çoklu sınıflandırmada anlamlı sonuçlar (%82.17 doğruluk) rapor etmiştir.

Erfani vd. (2021), IoT veri setlerini yatay ve dikey olarak zenginleştiren bir sistem geliştirerek Bot-IoT ve ToN-IoT veri setlerinde %99'un üzerinde F1-skorlar elde etmiştir. Jarjis vd. (2023), bu iki veri setini birlikte kullanarak XGB modeliyle %100 başarı elde etmiş, modelin üstün tespit gücünü ortaya koymuştur.

Bot-IoT veri seti üzerinde çalışan Leevy vd. (2021), bilgi hırsızlığı saldırılarının tespiti için çeşitli sınıflandırıcıları test etmiş, CatBoost ve XGBoost gibi topluluk modellerinin yüksek performans gösterdiğini belirtmiştir. Benzer şekilde, Saba vd. (2022), veri kümesinden az sayıda örneğe sahip saldırı türlerini çıkararak CNN ile %95.55 doğruluk elde etmiştir.

Swarna Sugi ve Ratna (2020), IoT ağlarındaki gizlilik sorunlarını ele alarak LSTM ve KNN temelli çözümler önermiş; tekrarlayan sinir ağlarının yüksek doğruluk sağladığını göstermiştir. Tarımsal IoT uygulamaları için Friha vd. (2022) tarafından geliştirilen FELIDS sistemi, klasik yöntemlere kıyasla daha üstün tespit sonuçları üretmiştir.

Yukarıda özetlenen literatürler incelendiğinde, IoT ağlarında saldırı tespiti için birçok başarılı yöntem geliştirildiği görülmektedir. Ancak mevcut çalışmaların büyük bir bölümü yalnızca statik veri setleri üzerinde gerçekleştirilmiş olup, gerçek zamanlı trafik analizine yeterince odaklanılmamıştır. Ayrıca, geliştirilen modellerin genellenebilirlik düzeylerinin düşük olması, bu sistemlerin farklı ortamlarda güvenilirliğini sınırlamaktadır. Bazı çalışmalar ağ trafiğini analiz ederek anormal davranışları saptamak amacıyla makine öğrenmesi tekniklerinden faydalansa da bu çözümler çoğunlukla yüksek donanım gereksinimi nedeniyle küçük ve orta ölçekli işletmeler için uygulanabilir değildir. Bu çalışma, söz konusu sınırlamaları aşmak amacıyla hem statik hem de canlı ağ trafiğini analiz edebilen, yapay zeka ve denetimli öğrenme temelli bir saldırı tespit sistemi önermektedir. Geliştirilen sistem, Raspberry Pi gibi düşük maliyetli cihazlarla uyumlu çalışabilmekte ve tespit edilen tehditleri kullanıcıya anlık bildirimler ile ileterek güvenlik farkındalığını artırmaktadır. Bu yönüyle çalışma, küçük ölçekli IoT altyapılarına sahip kurumlar için erişilebilir, ölçeklenebilir ve etkili bir çözüm sunmakta; literatürdeki önemli bir boşluğu doldurmaktadır.

## 3. Materyal ve Yöntem (Material and Method)

### 3.1. Veri Setinin Düzenlenmesi (Dataset Preparation)

Bu çalışmada kullanılan veri seti, IoT tabanlı ağ trafiğini temsil eden ve farklı saldırı türlerini içeren etiketli bir veri kümesidir. Veri seti, TCP, UDP, ACK ve CBR gibi çeşitli paket tiplerini ve 50'den fazla düğüm (cihaz) etkileşimini içermektedir. Veri kümesinde toplamda 30'dan fazla öznitelik bulunmakta olup, bu öznitelikler arasında paket boyutu, paket gecikmesi, gönderim ve alınma zamanları, kaynak ve hedef düğümler, bayt oranı, ortalama paket boyutu gibi hem sayısal hem kategorik bilgiler yer almaktadır (Jacobvs, 2025). Öznitelikler Tablo 1'de verilmiştir. Veri setinde saldırı sınıfları olarak Normal, UDP-Flood, Smurf, SIDDOS ve HTTP-FLOOD gibi çeşitli DDoS türleri tanımlanmıştır.

**Tablo 1.** Veri setinin öznitelikler (Features)

| Öznitelik | Türü | Açıklama |
|---|---|---|
| SRC_ADD | Numeric | Kaynak adresini temsil eder. |
| DES_ADD | Numeric | Hedef adresini belirtir. |
| PKT_ID | Numeric | Paketin benzersiz kimliği. |
| FROM_NODE | Numeric | Paketi gönderen düğüm numarası. |
| PKT_TYPE | Categorical | Paketin türü (örn. TCP, UDP). |
| PKT_SIZE | Numeric | Paketin boyutu (byte cinsinden). |
| FLAGS | Categorical | Protokole özgü bayrak bilgileri. |
| FID | Numeric | Akış kimliği (Flow ID). |
| SEQ_NUMBER | Numeric | Paketin sıra numarası. |
| NUMBER_OF_PKT | Numeric | Gönderilen paket sayısı. |
| NUMBER_OF_BYTE | Numeric | Gönderilen toplam byte miktarı. |
| NODE_NAME_FROM | Categorical | Gönderen düğümün adı. |
| NODE_NAME_TO | Categorical | Alıcı düğümün adı. |
| PKT_IN | Numeric | Düğüme gelen paket sayısı. |
| PKT_OUT | Numeric | Düğümlerden çıkan paket sayısı. |
| PKT_R | Numeric | Alınan paket sayısı. |
| PKT_DELAY_NODE | Numeric | Bir düğümdeki paket gecikmesi. |
| PKT_RATE | Numeric | Paket gönderim hızı. |
| BYTE_RATE | Numeric | Bayt gönderim hızı. |
| PKT_AVG_SIZE | Numeric | Paketlerin ortalama boyutu. |
| UTILIZATION | Numeric | Ağın kullanım oranı. |
| PKT_DELAY | Numeric | Toplam paket gecikmesi. |
| PKT_SEND_TIME | Numeric | Paketin gönderilme zamanı. |
| PKT_RESERVED_TIME | Numeric | Paketin ayrıldığı süre. |
| FIRST_PKT_SENT | Numeric | İlk gönderilen paketin zamanı. |
| LAST_PKT_RESERVED | Numeric | Son ayrılan paketin zamanı. |
| PKT_CLASS | Categorical | Paketin sınıfı (örn. kontrol, veri). |

Veri ön işleme sürecinde ilk olarak sayısal özniteliklerde yer alan bozuk veya eksik değerler tespit edilerek temizlenmiş; bu değerler, ilgili sütunun medyan değeriyle doldurulmuştur. Kategorik öznitelikler (ör. PKT_TYPE, NODE_NAME_FROM, NODE_NAME_TO) etiket kodlayıcılar (Label Encoder) yardımıyla sayısal forma dönüştürülmüştür. Ardından, verinin ölçeklenmesi için standartlaştırma (StandardScaler) yöntemi uygulanmıştır.

Veri dengesizliğini gidermek için, her bir saldırı sınıfı için maksimum 4000 örnekle sınırlı olacak şekilde örnekleme yapılmış; azınlık sınıflar çoğaltılmış, çoğunluk sınıflar ise dengelenmiştir. Bu dengeleme işlemi, veri kümesindeki sınıf dağılımını eşitleyerek modelin az temsil edilen saldırı türlerine karşı da yüksek performans göstermesini sağlamıştır. Böylelikle, model eğitimi için daha dengeli ve temsil gücü yüksek bir veri yapısı elde edilmiştir.

### 3.2. Sınıflandırma Modeli (Classification Model)

Bu çalışmada, IoT ağlarında gerçekleşen DDoS saldırılarını tespit etmek amacıyla denetimli öğrenme temelli bir sınıflandırma süreci gerçekleştirilmiştir. Sınıflandırma modellerinin doğruluğunu değerlendirmek ve genellenebilirliğini artırmak için eğitim sürecinde hem eğitim-test ayrımı hem de k-katlı çapraz doğrulama (k-fold cross-validation) yöntemi kullanılmıştır.

**K-Katlı Çapraz Doğrulama (K-Fold Cross-Validation):** Veri kümesinin rastgele olarak k eşit parçaya (katlara) ayrıldığı bir geçerleme tekniğidir. Her bir kat, sırasıyla test verisi olarak ayrılırken, kalan k−1 kat eğitim verisi olarak kullanılır. Bu işlem k kez tekrarlanır ve her bir tekrar için elde edilen model başarımı kayıt altına alınır. Tüm katlardaki sonuçların ortalaması alınarak modelin genel performansı hesaplanır. Bu yöntem, modelin yalnızca belirli bir veri kümesinde değil, genel dağılım üzerinde de başarılı olup olmadığını değerlendirmek için yaygın olarak kullanılmaktadır. Bu çalışmada k=5 olarak belirlenmiş ve beş katlı geçerleme uygulanmıştır. Böylece her bir örnek, bir kez test ve dört kez eğitim verisi olarak kullanılarak değerlendirme adil ve istikrarlı hâle getirilmiştir. Modelin başarımını değerlendirmek amacıyla çeşitli ölçütler kullanılmıştır (Kayaalp, 2024):

**Kesinlik (Precision):** Modelin pozitif olarak sınıflandırdığı örneklerin ne kadarının gerçekten pozitif olduğunu gösterir. Yanlış pozitif tahminleri azaltma gücünü ölçer.

$$Kesinlik = \frac{DP}{DP + YP} \quad (1)$$

**Duyarlılık (Recall):** Gerçek pozitif örneklerin ne kadarının doğru şekilde tahmin edildiğini ifade eder. Kaçırılan pozitif vakaları (FN) azaltma gücünü gösterir.

$$Duyarlılık = \frac{DP}{DP + YN} \quad (2)$$

**Özgüllük (Specificity):** Gerçek negatif sınıfların ne kadar doğru sınıflandırıldığını ifade eder. Modelin yanlış alarm üretmeden normal durumları tanıma kapasitesini ölçer.

$$Özgüllük = \frac{DN}{DN + DP} \quad (3)$$

**AUC (Area Under Curve):** ROC eğrisinin altında kalan alanı ifade eder. Pozitif ve negatif sınıflar arasındaki ayrım kapasitesini ölçer. AUC değeri 1'e ne kadar yakınsa, modelin ayırt etme gücü o kadar yüksek kabul edilir.

$$AUC \in [0.5, 1.0] \quad (4)$$

Bu metrikler, hem her bir çapraz doğrulama katı için hem de genel ortalama olarak hesaplanmıştır. Bu değerlendirmeler sayesinde modelin hem doğruluğu hem de farklı saldırı türlerini ayırt etme kapasitesi detaylı biçimde analiz edilmiştir. Elde edilen sonuçlar, çalışmanın sonraki bölümlerinde sayısal olarak sunulmaktadır.

#### 3.3.1. Algoritma Seçimi (Algorithm Selection)

Bu çalışmada, IoT ağlarındaki DDoS saldırılarını tespit edebilmek amacıyla farklı makine öğrenmesi tabanlı sınıflandırma algoritmaları değerlendirilmiştir. Her algoritmanın temel çalışma prensipleri, avantajları ve kullanım amacı göz önünde bulundurularak modelleme sürecine dahil edilmiştir. Aşağıda, çalışmada kullanılan başlıca sınıflandırma algoritmaları özetlenmektedir.

**Gaussian Naive Bayes:**

Gaussian Naive Bayes, olasılıksal sınıflandırma yöntemlerinden biri olup, Bayes teoremini temel alır ve öznitelikler (değişkenler) arasında koşulsuz bağımsızlık olduğunu varsayar. Bu modelde, her sınıfın olasılığı ve gözlemlenen verilerin her bir sınıfa ait olma olasılığı hesaplanarak, yeni örneklerin en olası sınıfa atanması sağlanır. Bu yaklaşım, modelin basit yapısına rağmen hızlı ve hafif olması sayesinde, özellikle büyük boyutlu ve yüksek değişkenli veri kümelerinde etkili sonuçlar elde edilmesini sağlar. Gaussian Naive Bayes, ön işleme maliyeti düşük, eğitim süresi kısa ve genel doğruluk oranı tatmin edici olan bir algoritma olarak, metin sınıflandırma, tıbbi teşhis ve ağ güvenliği gibi pek çok alanda tercih edilmektedir. Ancak öznitelikler arasında bağımlılık bulunması durumunda modelin performansı düşebilir. Ayrıca, normal dağılım varsayımının sağlanmadığı durumlarda sonuçların güvenilirliği azalabilir (Anand vd., 2022).

**Doğrusal Destek Vektör Sınıflandırıcı (Linear SVC):**

Linear SVC, destek vektör makinelerinin (SVM) doğrusal versiyonudur ve veri noktalarını en iyi şekilde ayıran hiper düzlemi bulmayı amaçlar. Bu hiper düzlem, sınıflar arasındaki marjini (sınır boşluğu) maksimize ederek modelin genellenebilirliğini artırır. Özellikle yüksek boyutlu, ancak doğrusal olarak ayrılabilir veri setlerinde oldukça etkilidir. Linear SVC, verilerin doğrusal olarak sınıflandırılabildiği durumlarda düşük hesaplama maliyeti ile hızlı ve kararlı sonuçlar üretir. Ancak, veriler doğrusal olmayan bir yapıya sahipse veya sınıflar karmaşık bir biçimde iç içe geçmişse, bu yöntem sınırlı kalabilir. Bu gibi durumlarda kernel tabanlı SVM yöntemleri tercih edilmektedir (Sanusi vd., 2022).

**Destek Vektör Makineleri (SVM):**

Destek Vektör Makineleri, sınıflar arasındaki ayrımı en iyi şekilde sağlayan karar sınırlarını öğrenmek için kullanılan güçlü bir denetimli öğrenme algoritmasıdır. SVM, yalnızca doğrusal ayrımları değil, aynı zamanda çekirdek (kernel) fonksiyonları aracılığıyla doğrusal olmayan ayrımları da başarıyla gerçekleştirebilir. Yaygın olarak kullanılan kernel türleri arasında polinomsal, radial basis function (RBF) ve sigmoid çekirdekleri yer alır. SVM, küçük ve orta ölçekli veri setlerinde yüksek doğruluk sağlayabilir ve özellikle sınıflar arasında net bir ayrımın olduğu durumlarda öne çıkar. Öte yandan, büyük veri setlerinde eğitimi daha yavaş olabilir ve kernel seçimi model performansını önemli ölçüde etkileyebilir (Chandra ve Bedi, 2021).

**Çok Katmanlı Algılayıcı (MLP):**

Çok Katmanlı Algılayıcı (MLP), yapay sinir ağlarının en temel yapı taşlarından biridir. MLP, bir giriş katmanı, bir veya daha fazla gizli katman ve bir çıkış katmanından oluşur. Her katmandaki nöronlar, kendisine gelen ağırlıklı girişleri aktivasyon fonksiyonu yardımıyla işler ve bir sonraki katmana aktarır. MLP, geri yayılım (backpropagation) algoritması ve gradyan iniş optimizasyonu ile öğrenme sürecini gerçekleştirir. Doğrusal olmayan ve karmaşık veri örüntülerini öğrenme kabiliyeti sayesinde, özellikle IoT gibi çok değişkenli ortamlarda yaygın biçimde tercih edilmektedir. Bununla birlikte, doğru mimari ve hiperparametrelerin seçimi kritik öneme sahiptir; aksi takdirde model aşırı öğrenme (overfitting) gösterebilir veya düşük performans sergileyebilir (Naskath vd., 2023).

**K-En Yakın Komşu (K-Nearest Neighbors - KNN):**

KNN, örneklerin sınıflandırılmasında en yakın komşularının sınıf bilgilerini dikkate alan tembel öğrenme (lazy learning) yöntemidir. Model, öğrenme aşamasında hiçbir işlem yapmaz; sınıflandırma işlemi, test örneğinin eğitim kümesindeki en yakın k komşusunun etiketlerine göre gerçekleştirilir. En sık kullanılan uzaklık ölçütü Öklidyen mesafe olmakla birlikte, Manhattan veya Minkowski mesafesi gibi alternatif metrikler de kullanılabilir. Yorumlanabilirliği yüksek ve implementasyonu basit olan bu yöntem, sınıflar arası belirgin sınırların olduğu küçük ve dengeli veri kümelerinde etkili sonuçlar vermektedir. Ancak yüksek boyutlu veya dengesiz veri kümelerinde performans kaybı yaşanabilir ve işlem süresi artabilir (Zhang vd., 2017).

**Aşırı Gradyan Artırma (XGBoost):**

XGBoost, gradyan artırma (gradient boosting) algoritmasının düzenleme (regularization) teknikleriyle geliştirilmiş bir versiyonudur. Temel olarak, her adımda hata yapan zayıf tahminleyicilerin (karar ağaçlarının) çıktısı üzerine yeni ağaçlar inşa edilerek güçlü bir sınıflayıcı oluşturulur. XGBoost'un dikkat çeken avantajları arasında, eksik verilerle başa çıkabilme, aşırı öğrenmeyi engelleme, paralel hesaplama desteği ve yüksek hesaplama verimliliği yer almaktadır. Bu özellikleri sayesinde, özellikle karmaşık, büyük ölçekli veri setlerinde üstün performans göstermektedir. IoT ağ güvenliği gibi çok katmanlı analizlerin gerekli olduğu durumlarda oldukça etkili bir modelleme aracı olarak öne çıkmaktadır *(Niazkar vd., 2024)*.

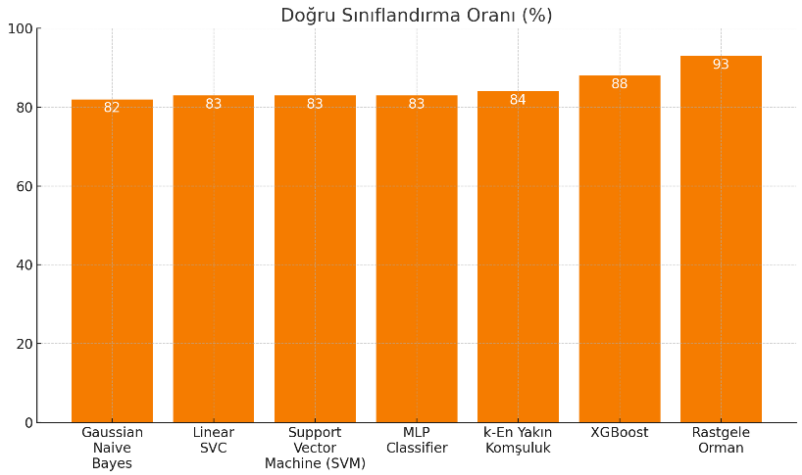
**Rastgele Orman (Random Forest):**

Random Forest, bagging (bootstrap aggregating) yöntemiyle oluşturulan çok sayıda karar ağacının çıktısını birleştiren bir topluluk (ensemble) öğrenme tekniğidir. Her bir ağaç, eğitim verisinin rastgele seçilmiş bir alt kümesi ve rastgele öznitelik alt kümeleriyle eğitilir. Nihai karar, ağaçların oy çoğunluğuyla belirlenir. Bu yapı, modelin aşırı öğrenmeye karşı dayanıklı olmasını ve farklı özniteliklerle gelen varyansın azaltılmasını sağlar. Random Forest, yüksek doğruluk oranı, açıklanabilirlik (özellik önem sıralaması) ve düşük parametre duyarlılığı ile sınıflandırma problemlerinde oldukça başarılıdır. Ancak çok sayıda ağaç oluşturulması nedeniyle hesaplama maliyeti artabilir (Hu ve Szymczak, 2023).

## 4. Deneysel Sonuçlar (Experimental Results)

Bu çalışmada geliştirilen DDoS saldırı tespit sisteminin başarımı, farklı makine öğrenmesi algoritmaları üzerinde değerlendirilmiş ve çeşitli metrikler kullanılarak karşılaştırılmıştır. Deneysel analizlerde, sınıflandırma modellerinin doğru sınıflandırma oranı, kesinlik (precision), duyarlılık (recall), özgüllük (specificity) ve AUC (Area Under Curve) skorları dikkate alınmıştır.

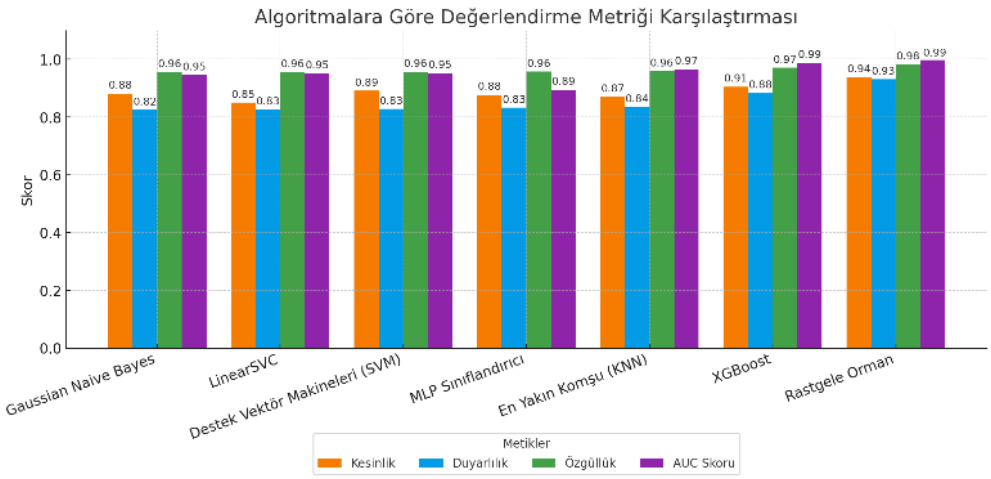
Bu çalışmada, DDoS tespit sistemi için yedi farklı makine öğrenmesi algoritmasının performansları kapsamlı bir şekilde değerlendirilmiştir. Algoritmaların doğru sınıflandırma oranları Şekil 3'te karşılaştırmalı olarak sunulmuştur. Sonuçlar incelendiğinde, Random Forest algoritmasının %93 doğruluk oranıyla en yüksek başarımı sergilediği görülmektedir. Bu algoritmanı sırasıyla XGBoost (%88), KNN (%84), Linear SVC (%83), SVM (%83), MLP (%83) ve Gaussian Naive Bayes (%82) takip etmektedir.




**Şekil 3.** Doğru sınıflandırma oranı (Classification accuracy rate)

Random Forest'ın üstün performansının temel nedeni, topluluk öğrenme (ensemble learning) yaklaşımının getirdiği avantajlardır. Bu algoritma, sınıf dağılımındaki dengesizliklere karşı daha dirençli bir yapıya sahip olup, birden fazla karar ağacının birleşik kararıyla sınıflar arası ayrımı daha başarılı şekilde gerçekleştirmektedir.

Doğruluk oranının yanı sıra, her algoritmanın çok boyutlu performansını değerlendirmek amacıyla dört temel metrik kullanılmıştır: kesinlik (precision), duyarlılık (recall), özgüllük (specificity) ve AUC (Area Under Curve) değeri. Bu metriklerin karşılaştırmalı analizi Şekil 4'te görselleştirilmiştir.




**Şekil 4.** Değerlendirme metriklerinin karşılaştırılması (Comparison of evaluation metrics)

Detaylı performans analizi sonuçları, Random Forest'ın tüm metriklerde tutarlı bir üstünlük sergilediğini ortaya koymaktadır. Bu algoritma, 0.99 AUC değeri ile mükemmel sınıf ayrım kapasitesi gösterirken, 0.94 kesinlik, 0.93 duyarlılık ve 0.98 özgüllük skorları ile dengeli bir performans sergilemektedir. XGBoost algoritması da benzer şekilde güçlü bir performans göstererek, 0.99 AUC skoru, 0.91 kesinlik ve 0.88 duyarlılık değerleriyle ikinci sırada yer almaktadır.

Daha basit algoritmalar arasında yer alan Gaussian Naive Bayes, 0.82 duyarlılık, 0.96 özgüllük ve 0.95 AUC değerleriyle genel olarak kabul edilebilir performans göstermiştir. Ancak doğruluk oranı ve kesinlik açısından topluluk öğrenme algoritmaları gerisinde kalmıştır. Linear SVC ve SVM algoritmaları ise yüksek AUC skorları (0.95) elde etmelerine rağmen, duyarlılık performansları 0.83 seviyesinde sınırlı kalmıştır.

Bu kapsamlı karşılaştırma sonuçları, özellikle çok sınıflı DDoS tespiti gibi karmaşık sınıflandırma problemlerinde topluluk öğrenme (ensemble learning) temelli algoritmaların üstünlüğünü açık şekilde ortaya koymaktadır. Random Forest ve XGBoost gibi modeller, hem yüksek doğruluk hem de model kararlılığı sağlayarak gerçek zamanlı uygulamalarda tercih edilmesi gereken çözümler olarak öne çıkmaktadır. Bu bulgular doğrultusunda, sistem performansı ve güvenilirlik açısından en optimal sonuçları veren Random Forest algoritması, geliştirilen DDoS tespit sisteminin nihai sınıflandırma modeli olarak seçilmiştir. Bu tercih, yalnızca doğruluk oranlarına değil; aynı zamanda eğitim sürecinde uygulanan teknik yapılandırmalara, çapraz doğrulama sonuçlarına ve modelin genel genellenebilirliğine dayanmaktadır.

Modelin eğitimi sürecinde, veri setindeki bozuk ve eksik değerler medyan ile doldurularak temizlenmiş; ardından logaritmik dönüşümler, oran bazlı hesaplamalar ve zaman serisi özellikleri gibi mühendislik süreçleri uygulanmıştır. Dengesiz sınıf yapısı, her sınıf için maksimum 4000 örnekle sınırlı olacak şekilde oversampling yöntemiyle dengelenmiş; böylece azınlıkta kalan saldırı türlerinin de etkili biçimde temsil edilmesi amaçlanmıştır.

Tablo 2, veri kümesindeki sınıf dağılımlarının eşitlenmeden önceki ve eşitlendikten sonraki durumlarını karşılaştırmalı olarak göstermektedir.

**Tablo 2.** Sınıf dağılımlarının dengeleme öncesi ve sonrası (Class distribution before and after balancing)

| Sınıf | Orijinal Sayı | Dengelenmiş Sayı |
|---|---|---|
| Normal | 1935959 | 4000 |
| UDP-Flood | 201344 | 4000 |
| Smurf | 12590 | 4000 |
| STDDOS | 6665 | 4000 |
| HTTP-FLOOD | 4110 | 4000 |

Random Forest modeli, IoT saldırı verileri üzerinde performans optimizasyonu amacıyla seçilmiş hiperparametrelerle eğitilmiştir. Modelde 200 adet karar ağacı (n_estimators=200) kullanılmış ve her ağacın derinliği max_depth=25 ile sınırlandırılmıştır; bu değerler, farklı kombinasyonlar denenerek ve 5-katlı Stratified K-Fold Cross Validation yöntemiyle performans analiz edilerek belirlenmiştir. Özellik seçimi, her düğüm bölünmesinde toplam özellik sayısının karekökü kadar olacak şekilde (max_features='sqrt') yapılmış ve sınıf dengesizlikleri için class_weight='balanced_subsample' seçeneği uygulanmıştır. Modelin doğruluk ve tutarlılığı, cross-validation sonuçlarıyla değerlendirilmiş ve ortalama doğruluk oranı %93 olarak ölçülmüştür. Son olarak, final model tüm veriler üzerinde yeniden eğitilerek kalıcı hâle getirilmiştir.

Seçilen Random Forest modelinin sınıflandırma performansı, Şekil 5'te sunulan karmaşıklık matrisi (confusion matrix) ile detaylı olarak analiz edilmiştir. Matris sonuçları, modelin çoğunlukla doğru sınıflandırma yaptığını ve özellikle Normal, HTTP-FLOOD ve UDP-Flood kategorilerinde yüksek isabet oranları elde ettiğini göstermektedir.

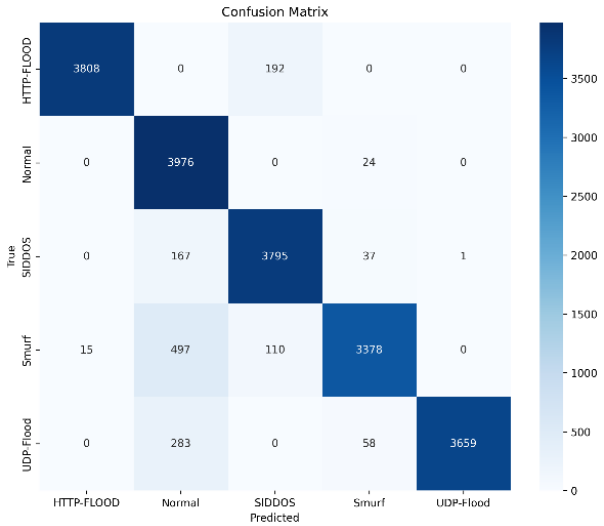
Karmaşıklık matrisinde Smurf saldırılarında gözlemlenen görece yüksek hata oranı, ROC eğrisinde de belirgin bir farklılık yaratmaktadır. Bunun temel nedeni Smurf saldırılarının ICMP flood tabanlı yapısı nedeniyle diğer DDoS türleriyle oldukça benzer trafik desenleri üretmesidir. Bu benzerlik, modelin Smurf ile diğer saldırı türlerini ayırt etmesini zorlaştırarak ROC eğrisinde daha fazla yanlış pozitif ve yanlış negatif sonuçlara yol açmaktadır. Ayrıca kullanılan özellik setinin Smurf saldırılarına özgü belirgin farklılıkları yeterince yakalayamaması ve eğitim verisinde Smurf örneklerinin diğer saldırı tiplerine göre daha az veya dengesiz bulunması da bu performans düşüşünü destekleyen etkenlerdir. Ancak tüm bu nedenlere rağmen AUC değerinin %99'un üzerinde olması, modelin genel başarımının yüksek olduğunu ve Smurf sınıfındaki kısmi zayıflığın sistemin bütünsel güvenilirliğini tehdit etmediğini göstermektedir.

Modelin her bir sınıf için ayrım kapasitesinin değerlendirilmesi amacıyla ROC eğrisi analizi gerçekleştirilmiştir. Şekil 6'da sunulan ROC eğrileri ve AUC değerleri, modelin sınıflar arası ayrım performansının detaylı bir resmini sunmaktadır.

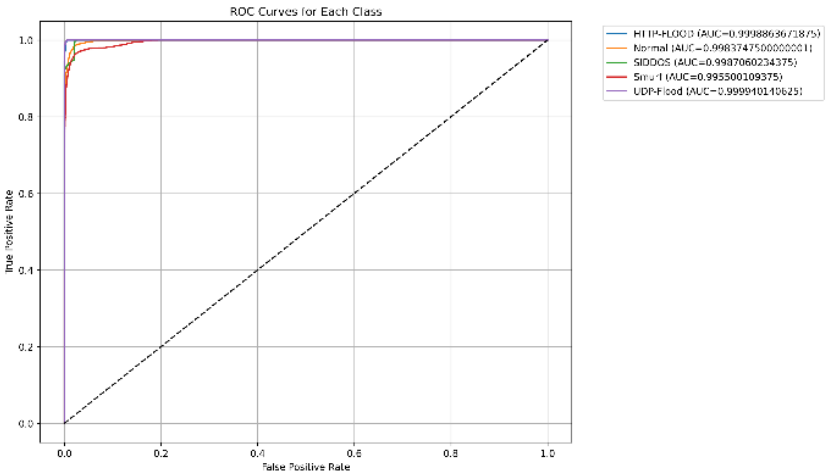
ROC eğrisi analizi sonuçları, modelin tüm sınıflarda mükemmel düzeyde performans sergilediğini ortaya koymaktadır. HTTP-FLOOD (0.9998), UDP-Flood (0.9999) ve Normal (0.9983) sınıfları için elde edilen AUC

değerleri, modelin bu kategorilerde neredeyse hatasız sınıflandırma yaptığını göstermektedir. Tüm sınıflar için AUC skorlarının 0.99 seviyesinde olması, Random Forest modelinin farklı saldırı türlerini güvenilir şekilde ayırt edebildiğini kanıtlamaktadır.

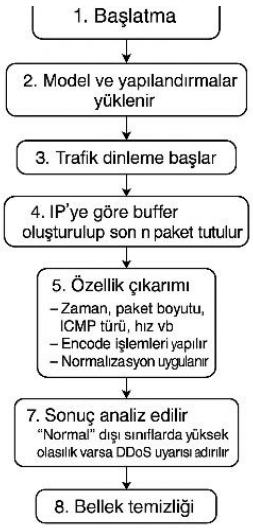
Bu yüksek performans sonuçları doğrultusunda, gerçek zamanlı DDoS tespit sistemi geliştirilmiştir. Sistemin çalışma mantığı ve işleyiş süreci Şekil 7'de akış diyagramı ile gösterilmiştir.




**Şekil 5.** Modelin karmaşıklık matrisi (Confusion matrix of the model)




**Şekil 6.** Modele ait ROC eğrileri (ROC curves of the model)




**Şekil 7.** Tespit sistemi akış diyagramı (Detection system flow diagram)

Geliştirilen gerçek zamanlı tespit sistemi, canlı ağ trafiğini sürekli analiz ederek potansiyel DDoS saldırılarını tespit etmek üzere tasarlanmıştır. Sistemin işleyiş süreci aşağıdaki adımlardan oluşmaktadır:

**Sistem Başlatma ve Model Yükleme:** Sistem başlangıcında, eğitim sürecinde oluşturulan ddos_model.joblib dosyası ve ilişkili ölçekleyici, kodlayıcı bileşenleri belleğe yüklenmektedir. Bu adım, sistemin tespit kapasitesinin hazır hale getirilmesi için kritik öneme sahiptir.

**Trafik Dinleme ve Paket Toplama:** Scapy kütüphanesi kullanılarak ağ arayüzü üzerinden geçen IP paketleri gerçek zamanlı olarak dinlenmektedir. Her IP adresi için ayrı buffer yapıları (deque) oluşturularak, son n adet paket bellekte tutulmaktadır.

**Özellik Çıkarımı ve Normalize Etme:** Belirli zaman aralıklarında, buffer içerisindeki paketlerden istatistiksel özellikler çıkarılmaktadır. Bunlar arasında paketler arası zaman farkları, ortalama gecikme süreleri ve byte oranları gibi özellikler yer almaktadır. Çıkarılan özellikler, model eğitiminde kullanılan standartlara uygun şekilde normalize edilmektedir.

**Model Tahmin ve Karar Verme:** Hazırlanan özellik vektörü, Random Forest modeline girdi olarak verilmekte ve her sınıf için olasılık değerleri üretilmektedir. Sistem, "Normal" sınıf dışındaki herhangi bir sınıf için olasılık değerinin önceden belirlenen eşik değerini aşması durumunda DDoS uyarısı vermektedir.

**Sistem Optimizasyonu:** İşlem tamamlandıktan sonra, geçici veriler ve bellek içeriği Python'ın gc modülü kullanılarak temizlenmekte ve sistem performansı korunmaktadır.

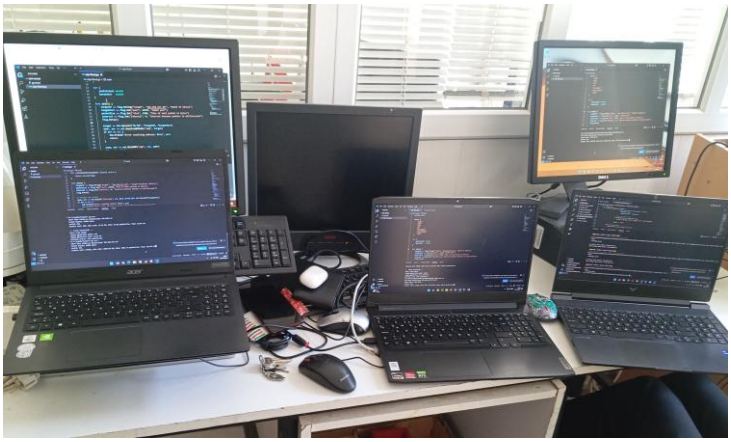
Bu sistematik yaklaşım sayesinde, IoT tabanlı ağ ortamlarında sürekli trafik izleme, saldırı desenlerinin zamanında tanınması ve gerçek zamanlı kullanıcı uyarısı mümkün kılınmıştır. Random Forest modelinin %93 doğruluk oranı ve 0.99 AUC skoru, sistemin farklı DDoS saldırı türlerini güvenilir şekilde tespit edebildiğini ve pratik uygulamalarda kullanılabilir düzeyde performans sergilediğini kanıtlamaktadır.

Geliştirilen sistem, erişim noktası (Access Point) olarak yapılandırılan Şekil 8'de gösterilen Raspberry Pi 3 cihazına entegre edilmiştir. Bu yapılandırma sayesinde Raspberry Pi, yalnızca bir işlem birimi olarak değil, aynı zamanda bir ağ geçidi (gateway) işlevi de görerek sistemin merkezinde konumlandırılmıştır. Sisteme bağlanan istemci cihazlardan gelen tüm ağ trafiği bu cihaz üzerinden yönlendirilmekte; bu trafik, arka planda kesintisiz çalışan gerçek zamanlı izleme modülü tarafından sürekli analiz edilmektedir. Böylece, herhangi bir ek donanıma ihtiyaç duyulmaksızın, düşük maliyetli, taşınabilir ve enerji açısından verimli bir donanım platformu üzerinde gerçek zamanlı DDoS saldırı tespiti mümkün hâle gelmektedir.

**Şekil 8.** Sistemin Raspberry Pi'a entegrasyonu (System integration into Raspberry Pi)

Sistem kurulumunun ardından, UDP-Flood, HTTP-Flood ve Smurf gibi farklı DDoS saldırı senaryoları Şekil 9'da gösterildiği gibi simüle edilerek platformun işlevselliği ve saldırı tespit yetenekleri kapsamlı şekilde test edilmiştir. Gerçekleştirilen deneysel çalışmalar neticesinde, sistemin hem normal ağ trafiğini hem de anormal/saldırgan trafiği başarılı bir şekilde sınıflandırabildiği; ayrıca, tespit edilen tehditlere ilişkin kullanıcıyı anlık olarak uyarabildiği gözlemlenmiştir.

Sunulan mimari yaklaşım, düşük donanım gereksinimi ve yazılım tarafında sahip olduğu modüler yapı sayesinde; küçük ve orta ölçekli işletmeler, bireysel kullanıcılar ve endüstriyel IoT uygulamaları için ekonomik, ölçeklenebilir ve güvenli bir ağ izleme çözümü sunmaktadır. Bu yönleriyle sistem, ticarileştirilmeye uygun, pratik ve yenilikçi bir güvenlik altyapısı olarak öne çıkmaktadır.



**Şekil 9.** Gerçek-zamanlı test düzeneği (Real-time test setup)

## 5. Sonuç ve Tartışma (Result and Discussion)

Bu çalışmada, IoT tabanlı ağlarda gerçekleşen DDoS saldırılarının tespitine yönelik, denetimli öğrenme ve yapay zeka tekniklerine dayalı bir saldırı tespit sistemi geliştirilmiştir. Geliştirilen model, hem statik veri setleri üzerinde hem de gerçek zamanlı ağ trafiğiyle test edilmiştir. Modelin doğruluk, kesinlik, duyarlılık ve AUC skoru gibi temel performans metriklerinde yüksek başarı oranlarına ulaştığı gözlemlenmiştir. Ayrıca, sistemin düşük maliyetli cihazlarla (örneğin Raspberry Pi) uyumlu çalışabilir olması, çözümün pratikte uygulanabilirliğini artırmakta ve küçük ölçekli işletmeler için erişilebilir bir alternatif sunmaktadır.

Çalışmada yalnızca saldırı tespiti sağlanmakta olup, tespit edilen tehditler kullanıcıya anlık olarak bildirilmektedir. Bu yönüyle sistem, doğrudan müdahale etmese de güvenlik farkındalığını artırmakta ve olası tehditlere karşı hızlı reaksiyon alınmasına olanak tanımaktadır.

Gelecek çalışmalar kapsamında, önerilen sistemin federated learning veya transfer learning gibi daha ileri düzey yapay zeka yaklaşımları ile güçlendirilmesi planlanmaktadır. Ayrıca, saldırı sonrası otomatik yanıt mekanizmalarının entegre edilmesi ve sistemin farklı IoT veri setleriyle genellenebilirliğinin daha kapsamlı olarak test edilmesi, araştırmanın bir sonraki adımını oluşturmaktadır. Bu sayede, sistemin hem tespit hem de müdahale kapasitesi geliştirilebilir ve daha kapsamlı bir güvenlik çözümüne dönüştürülebilir.

## Çıkar Çatışması (Conflict of Interest)

Yazarlar tarafından herhangi bir çıkar çatışması beyan edilmemiştir. No conflict of interest was declared by the authors.

## Kaynaklar (References)


Anand, M. V., KiranBala, B., Srividhya, S. R., Younus, M., Rahman, M. H., 2022. Gaussian Naïve Bayes algorithm: a reliable technique involved in the assortment of the segregation in cancer. Mobile Information Systems, 2022(1), 2436946, https://doi.org/10.1155/2022/2436946.

Bıçakçı, S. N., 2019. Nesnelerin interneti. Takvim-i vekayi, 7(1), 24-36.

Booij, T. M., Chiscop, I., Meeuwissen, E., Moustafa, N., Den Hartog, F. T., 2021. ToN_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets. IEEE Internet of Things Journal, 9(1), 485-496, doi: 10.1109/JIOT.2021.3085194.

Chandra, M. A., Bedi, S. S., 2021. Survey on SVM and their application in image classification. International Journal of Information Technology, 13(5), 1-11, https://doi.org/10.1007/s41870-017-0080-1.

DDoS attack network logs dataset, www.kaggle.com, [Online]. Available: https://www.kaggle.com/jacobvs/ddos-attack-network-logs (Erişim 28 Mayıs 2025)

Erfani, M., Shoeleh, F., Dadkhah, S., Kaur, B., Xiong, P., Iqbal, S., Ghorbani, A. A., 2021. A feature exploration approach for IoT attack type classification. In 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 582-588). IEEE, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech52372.2021.00101.

Friha, O., Ferrag, M. A., Shu, L., Maglaras, L., Choo, K. K. R., Nafaa, M., 2022. FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things. *Journal of Parallel and Distributed Computing*, *165*, 17-31, https://doi.org/10.1016/j.jpdc.2022.03.003.

Ghosh, A., Chakraborty, D., Law, A., 2018. Artificial intelligence in Internet of things. CAAI Transactions on Intelligence Technology, 3(4), 208-218, https://doi.org/10.1049/trit.2018.1008.

Hu, J., Szymczak, S., 2023. A review on longitudinal data analysis with random forest. Briefings in bioinformatics, 24(2), bbad002, https://doi.org/10.1093/bib/bbad002.

Jarjis, A. H., Al Zubaidi, N. Y. S., Pehlivanoglu, M. K., 2023. Cyber Attacks Classification on Enriching IoT Datasets. EAI Endorsed Transactions on Internet of Things, 9(3). DOI:10.4108/eetiot.v9i3.3030.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., Qiu, D., 2014. Security of the Internet of Things: perspectives and challenges. Wireless networks, 20, 2481-2501, https://doi.org/10.1007/s11276-014-0761-7.

Kayaalp, K., 2024. Classification of medicinal plant leaves for types and diseases with hybrid deep learning methods. Information Technology and Control, 53(1), 19-36, https://doi.org/10.5755/j01.itc.53.1.34345.

Kurtoğlu, E., Süslü, D. P., 2024. Türkiye'de internet bağımlılığı ile ilgili yapılmış lisansüstü tezlerin incelenmesi. Bağımlılık Dergisi, 25(1), 10-22, https://doi.org/10.51982/bagimli.1246529.

Leevy, J. L., Hancock, J., Khoshgoftaar, T. M., Peterson, J., 2021. Detecting Information Theft Attacks in the Bot-IoT Dataset. Proceedings - 20th IEEE International Conference on Machine Learning and Applications, ICMLA 2021: 807–812. https://doi.org/10.1109/ICMLA52953.2021.00133

Mercan, Ö. B., Toprak, A. G., Osmanca, M. S., 2025. IoT saldırı algılaması için çok sınıflı sınıflandırma: LLM tabanlı bir yaklaşım. 2025 yılında 33. Sinyal İşleme ve İletişim Uygulamaları Konferansı (SIU) (s. 1-4). IEEE.

Mohanta, B. K., Jena, D., Satapathy, U., Patnaik, S., 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227. https://doi.org/10.1016/j.iot.2020.100227.

Naskath, J., Sivakamasundari, G., Begum, A. A. S., 2023. A study on different deep learning algorithms used in deep neural nets: MLP SOM and DBN. Wireless personal communications, 128(4), 2913-2936, https://doi.org/10.1016/j.envsoft.2024.105971.

Niazkar, M., Menapace, A., Brentan, B., Piraei, R., Jimenez, D., Dhawan, P., Righetti, M., 2024. Applications of XGBoost in water resources engineering: A systematic literature review (Dec 2018–May 2023). Environmental Modelling & Software, 174, 105971, https://doi.org/10.1016/j.envsoft.2024.105971.

Ntayagabiri, J. P., Bentaleb, Y., Ndikumagenge, J., El Makhtoum, H., 2025. A comparative analysis of supervised machine learning algorithms for IoT attack detection and classification. *Journal of Computing Theories and Applications, 2*(3), 395-409, https://doi.org/10.62411/jcta.11901.

Saba, T., Rehman, A., Sadad, T., Kolivand, H., Bahaj, S. A., 2022. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering, https://doi.org/10.1016/J.COMPELECENG.2022.107810 99.

Sahu, A. K., Sharma, S., Tanveer, M., Raja, R., 2021. Internet of Things attack detection using hybrid Deep Learning Model. Computer Communications, 176, 146-154, https://doi.org/10.1016/j.comcom.2021.05.024.

Sanusi, T. R., Andreas, F., Sari, B. N., 2022. Implementasi Algoritma Support Vector Classifier (SVC) dengan Data Training Numerik dan Teks untuk Mengklasifikasi SMS Spam. Jurnal Ilmiah Wahana Pendidikan, 8(14), 346-354, https://doi.org/10.5281/zenodo.6994895.

Swarna Sugi, S. S., Ratna, S. R., 2020. Investigation of machine learning techniques in intrusion detection system for IoT network. Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, 1164–1167. https://doi.org/10.1109/ICISS49785.2020.9315900

Turak, Y., 2015. Nesnelerin interneti ve güvenliği. Bilişim Teknolojisi Hukuku Enstitüsü, Bilişim Hukuku Anabilim Dalı, İstanbul Bilgi Üniversitesi, 3.

Ullah, I., Mahmoud, Q. H., 2021. Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access, 9, 103906-103926, doi: 10.1109/ACCESS.2021.3094024.

Woźniak, M., Siłka, J., Wieczorek, M., Alrashoud, M., 2020. Recurrent neural network model for IoT and networking malware threat detection. IEEE Transactions on Industrial Informatics, 17(8), 5583-5594, doi: 10.1109/TII.2020.3021689.

Zhang, S., Li, X., Zong, M., Zhu, X., Cheng, D., 2017. Learning k for knn classification. ACM Transactions on Intelligent Systems and Technology (TIST), 8(3), 1-19, https://doi.org/10.1145/2990508.