

Hazırlayan Emir Çağlar

**-Yapay Zeka ile
Siber Tehdit
Tespiti**



Yapay zekanın siber güvenlikteki rolü

AI sistemleri, büyük veri setlerini hızla analiz ederek, insan analistlerin tespit etmeye zorlanacağı tehditleri kısa sürede fark edebiliyor

Tehdit tespitinde kullanılan yapay zeka algoritmaları, makine öğrenmesi ve derin öğrenme teknikleriyle ağ trafiği, kullanıcı davranışları ve sistem loglarını tarayarak anomalî ve saldırı girişimlerini tespit ediyor.



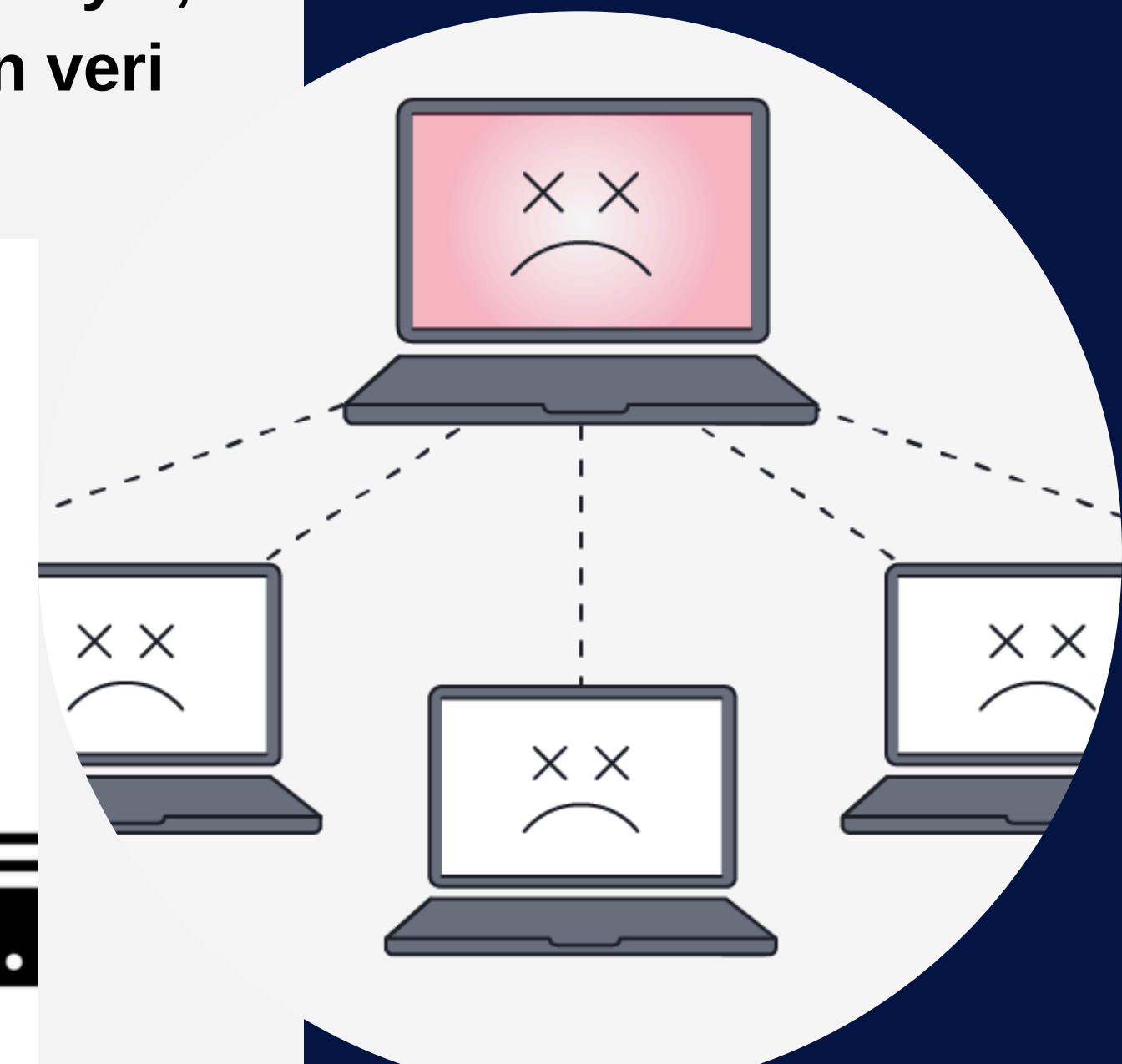
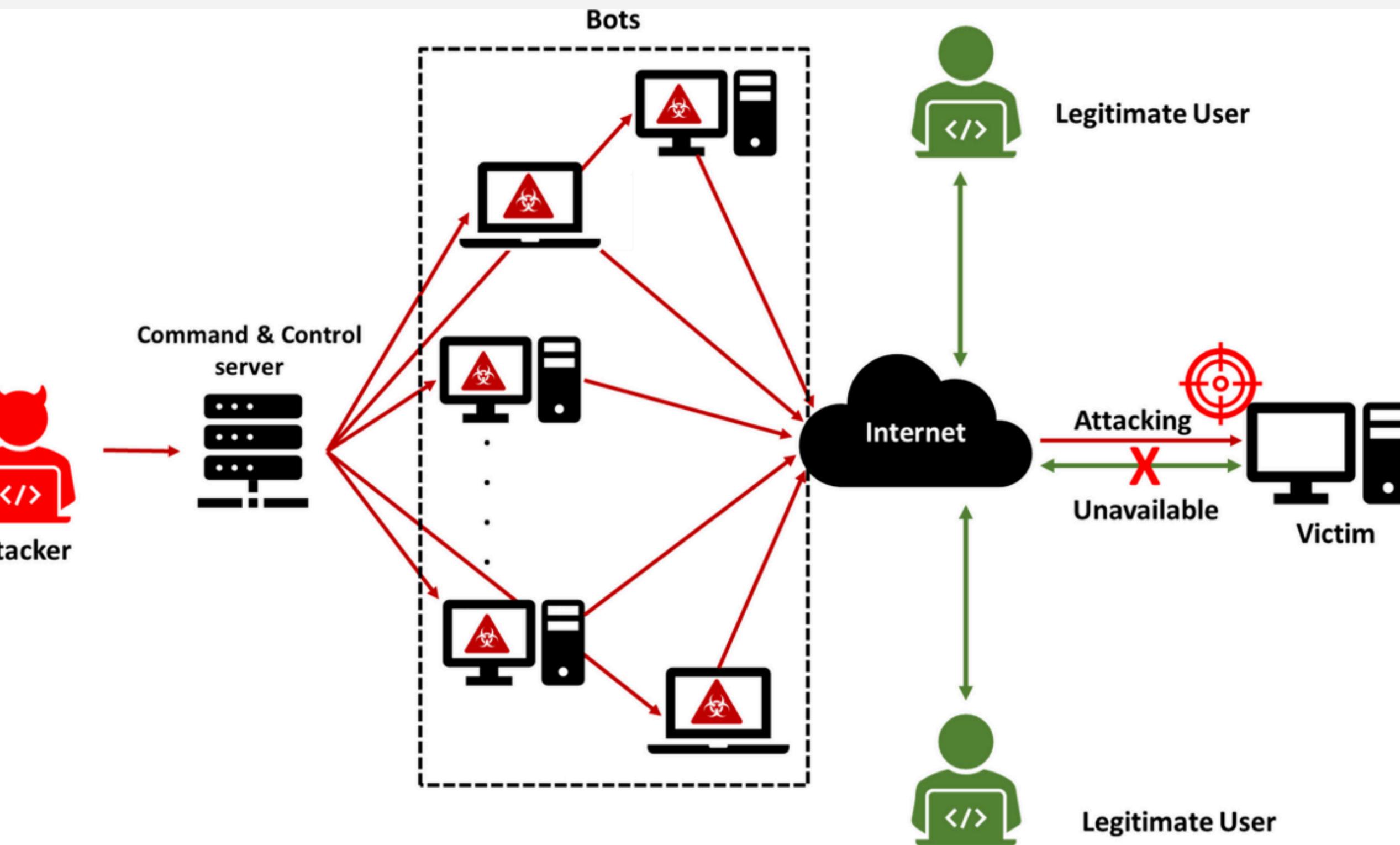
Yapay zekanın farklı türdeki siber saldırıları tespit etme doğruluğu

Saldırı Türü	Tahmin Doğruluğu (Ortalama)	Açıklama
DDoS (Dağıtık Hizmet Reddi Saldırısı)	%95 - %98	Yapay zeka, ağ trafiğindeki anormallikleri ve yoğun artışları oldukça yüksek doğrulukla tespit eder.
Kimlik Doğrulama Saldırıları	%92 - %96	AI, kullanıcı davranışlarındaki şüpheli değişiklikleri izleyerek kimlik saldırısını tanıyalabilir.
Zararlı Yazılım Saldırıları	%85 - %90	AI, dosya davranışlarını analiz ederek zararlı yazılım içeriklerini doğru tespit edebilir.
Sosyal Mühendislik Saldırıları (Phishing)	%80 - %85	E-postalar ve sosyal mühendislik içerikli saldırılarda düşük oranlarda tespit edilebilir.
SQL Injection Saldırıları	%88 - %93	Veritabanı sorgularındaki anormallikler yüksek oranda tespit edilir.
Sıfır Gün Saldırıları	%70 - %75	Bu saldırılar daha az bilinen tehditler olduğundan, tespit oranı daha düşüktür.



Örnek Problem: DDoS (servis dışı bırakma) Saldırı Tespiti

DoS saldırısı, bir ağın veya sistemin performansını bozmak amacıyla, çeşitli kaynaklardan (botnet veya kötü amaçlı yazılımlar) yoğun veri trafiği gönderilerek yapılan bir saldırıdır.



Yapay Zekaya Nerede İhtiyacımız Olacak?

- Web siteleri ve uygulamalar
- E-ticaret platformları
- Bankacılık ve finans kurumlarının dijital sistemleri
- Kamuya açık servisler, API'ler, bulut platformları

Hangi Eksiklikleri Engelleyecek?

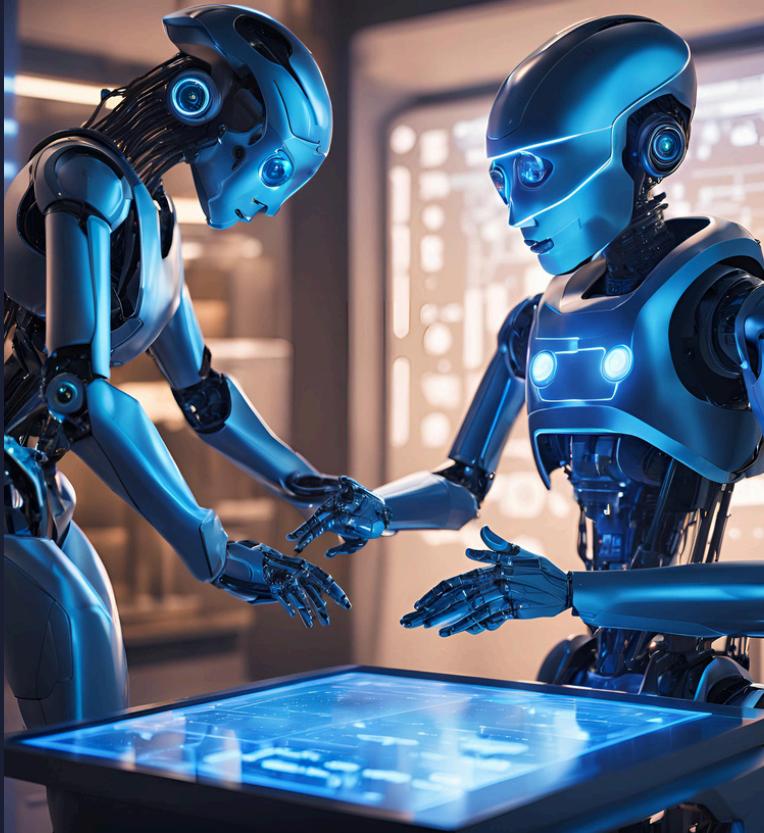
- DDoS saldırıları nedeniyle kesintiler ve veri kayıpları
- Aşırı ağ trafiği nedeniyle sistemlerin çökmesi.
- Sunucu ve ağ altyapısına verilen zararın önlenmesi.



Model Mantığı

DDoS saldırısı tespitinde kullanılan makine öğrenimi modelleri, ağ trafiğini analiz eder

1. Ağ trafiğinden elde edilen verilerle normal ve anormal (saldırı) trafik desenleri arasında farklar öğrenilir.
2. Trafikteki farklı özelliklere (paket sayısı, IP adresi, port numaraları, protokoller vb.) bakılarak saldırı tespit edilir.
3. Model, yeni gelen trafik için sınıflandırma yaparak, bu trafiğin normal mi yoksa saldırı mı olduğunu belirler.



Veri Seti ve Özellikleri

Özellik	Açıklama					
IP Adresi	Trafiğin hangi IP adresinden geldiği					
Protokol	TCP, UDP gibi kullanılan protokoller					
Paket Sayısı	Belirli bir süre zarfında gönderilen paket sayısı					
Bağlantı Süresi	Her bir bağlantının süresi					
Hedef Portu	Trafiğin hedef aldığı port numarası					
Veri Miktari	Gönderilen veri miktarı (byte cinsinden)					
Paket Boyutu	Gönderilen paketlerin boyutları					
Zaman Damgası	Trafiğin gönderildiği zaman					
Kaynak IP Sayısı	Trafiği gönderen farklı IP sayısı (saldırılarda bu sayı artabilir)					
Örnek veri:						
IP Adresi	Protokol	Paket Sayısı	Bağlantı Süresi	Hedef Portu	Veri Miktari (byte)	Paket Boyutu (byte)
192.168.1.1	TCP	50	2ms	80	1500	30
192.168.1.2	UDP	100	3ms	53	2000	40
...



Model Nasıl Oluşturulur?

DDoS saldırısını tespit etmek için aşağıdaki adımlar izlenir

Veri Ön İşleme

Özellik Seçimi

Model Seçimi

Veriler temizlenir, eksik veya hatalı veriler düzelttilir. Veri seti normalleştirilir, ağ trafiği genellikle çok büyük ölçeklerde olduğu için bu adım önemlidir

Trafiğin analiz edilebilmesi için gerekli olan önemli özellikler seçilir. Ağırlıklı olarak paket sayısı, veri miktarı, bağlantı süresi, hedef portu ve protokoller gibi veriler dikkate alınır.

DDoS saldırıları, sınıflandırma problemleri olarak modelleme yapılabilir. Bunun için Random Forest, SVM veya XGBoost gibi algoritmalar kullanılabilir

Modelimi Random Forest olarak seçtim ve eğittim

Random Forest, bir topluluk öğrenme yöntemidir ve birçok karar ağacından oluşur

```
24  
25 # 5. Random Forest modelini oluşturma ve eğitme  
26 model = RandomForestClassifier(n_estimators=100, random_state=42)  
27 model.fit(X_train, y_train)
```

Burada, Random Forest modelini 100 adet karar ağacı ile oluşturuyoruz. Bu, modelin kararlarını 100 farklı ağacın tahminlerinin ortalaması olarak almasını sağlar.

random_state=42 parametresi, Bu modelin sonuçlarının yeniden üretilebilir olmasını sağlar.

model.fit(X_train, y_train): Bu satır, modelin eğitim verisi üzerinde öğrenmesini sağlar.

X_train özellikleri (input verisi), y_train ise etiketler (gerçek sonuçlar) temsil eder.

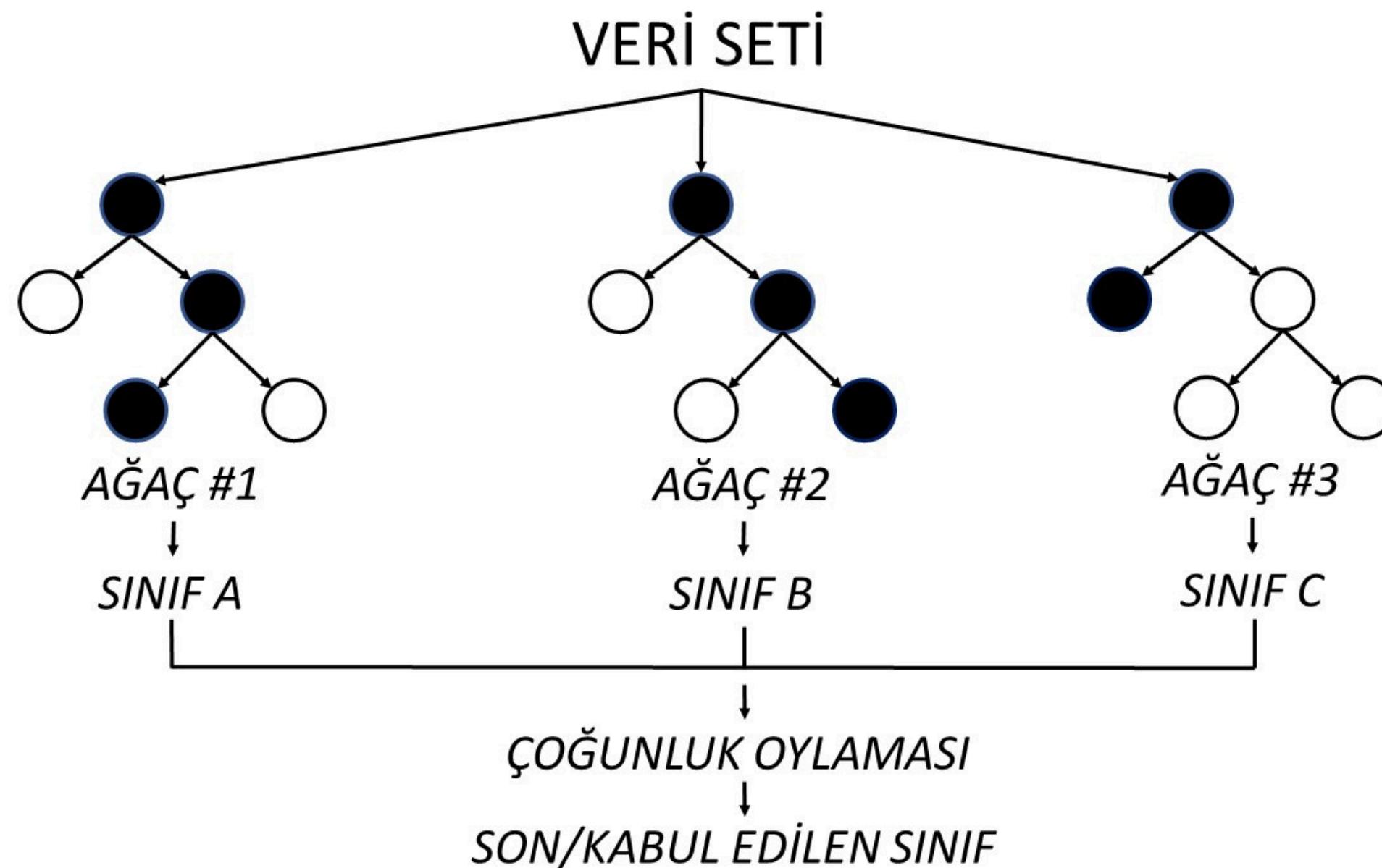
Modeli Neden Random Forest seçtiğimiz?

Yüksek Doğruluk: Birden fazla karar ağacını birleştirerek overfitting (aşırı uyum) riskini azaltır.

Kolay Genelleme: Random Forest genellikle küçük veya büyük veri setleriyle etkili bir şekilde çalışır

Özellik Seçimi: Random Forest, özellikle veri setindeki önemli özellikleri belirleme konusunda faydalıdır.

Daha Az Parametre Ayarlaması Gereksinimi: onu pratik hale getirir.



Çıktılar

- **Doğruluk Oranı (Accuracy):** Modelin doğru sınıflandırdığı trafik oranı.
- **Precision ve Recall:** DDoS saldırılarının ne kadar doğru tespit edildiğini gösterir.
- **Karmaşa Matrisi:** Gerçek pozitif, yanlış pozitif, gerçek negatif ve yanlış negatif değerlerini gösteren matris
- **F1 Skoru:** Kesinlik ve duyarlılığın birleşimi olarak modelin genel başarısını ölçen metrik.

Accuracy: 0.95

Precision: 0.93

Recall: 0.92

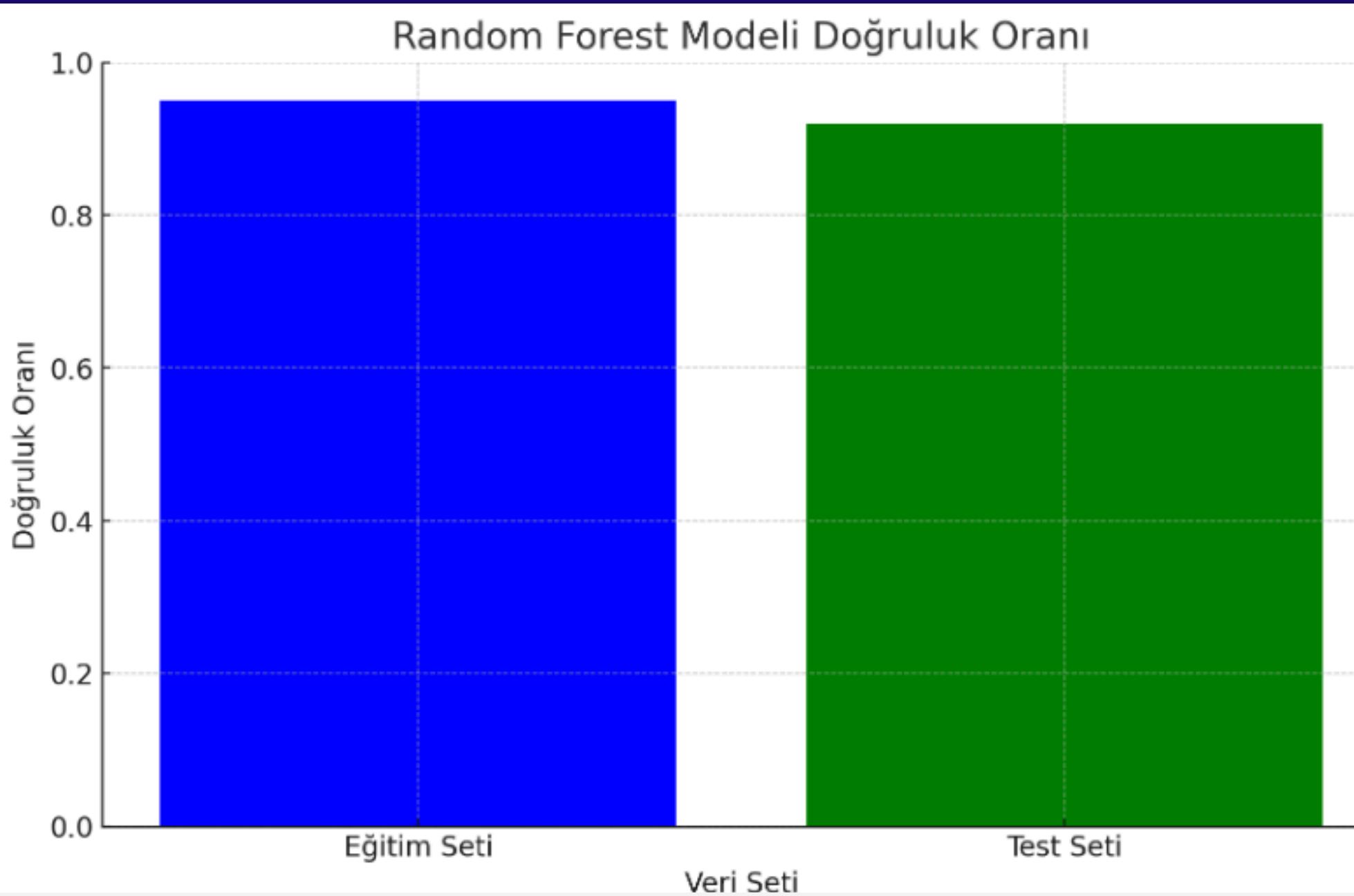
F1 Score: 0.92

Confusion Matrix:

[[500	10]
	[20	470]

Eğer eğitim doğruluğu test doğruluğundan çok daha yüksekse, model overfitting yapmış olabilir, yani model eğitim verisine çok fazla uyum sağlamakta ancak yeni verilere genelleme yapamamaktadır.

Eğitim ve test doğrulukları benzerse, model genellikle daha iyi bir şekilde genellenebilir.



Mavi çubuk, eğitim seti üzerindeki doğruluk oranını (%95)

Yeşil çubuk ise test seti üzerindeki doğruluk oranını (%92) temsil etmektedir.