# Çeşitli Özellikleri Kullanan Android IoT Cihazları için Çok Amaçlı Zararlı Yazılım Algılama Teknikleri

Kamil Akarsu
*Manisa Celal Bayar Üniversitesi, Yazılım Mühendisliği Yüksek Lisans*
*Turgutlu/ Manisa*
*191201005@ogr.cbu.edu.tr*

**Özet:** Son zamanlarda, nesnelerin interneti (IoT) sağlık, akıllı tarım, akıllı ev, akıllı alışveriş, vb. gibi çeşitli uygulamaların tanıtılmasıyla genişlemektedir[1]. Paylaşılan bir IoT ağındaki cihazlar, sensör arayüzü için çok önemli olan esneklik, sağlamlık ve donanım desteği nedeniyle Android platformuna dayanmaktadır. Nesnelerin İnterneti (IoT); algılayıcı-önleyici sistemler, sağlık hizmeti, uzaktan kontrol ve görüntüleme gibi hayatımızın çeşitli alanlarında geliştirilen uygulamalarla dünyada devrim yaratmaktadır. Bu hizmetleri sağlarken en büyük desteği Android cihazlar ve uygulamalardan görmektedir. Android tabanlı cihazlarda tehtit ve kötü amaçlı yazılım saldırılarında hızlı bir artış gözlenmektedir. IoT cihazlarındaki Android platformunun kapsamlı bir şekilde kullanılması nedeniyle zararlı yazılım etkinliklerinin önlenmesi gerekmektedir.

## 1. Giriş

Bu makale, Android IoT cihazlarının kötü amaçlı yazılım tespitini iyileştirmek için hem Makine Öğrenmesi tekniklerinin hem de Blok Zinciri teknolojisinin avantajlarını birleştiren yeni bir çerçeve sunmaktadır. Önerilen teknikler, kümeleme, sınıflandırma ve Blok Zinciri içeren sıralı bir yaklaşım kullanılarak uygulanır.[2] Makine Öğrenmesi, kümeleme ve sınıflandırma tekniğini kullanarak kötü amaçlı yazılım bilgilerini otomatik olarak çıkarır ve bilgileri Blok Zincirinde saklar. Böylece, Blok Zinciri geçmişinde depolanan tüm kötü amaçlı yazılım bilgileri ağ üzerinden iletilebilir ve bu nedenle kötü amaçlı yazılımlar etkili bir şekilde tespit edilebilir. Kümeleme tekniğinin uygulanması, her özellik kümesi için ağırlıkların hesaplanmasını, optimizasyon için parametrik çalışmanın geliştirilmesini ve aynı anda küçük ağırlıklara sahip gereksiz özelliklerin yinelemeli olarak azaltılmasını içerir. Sınıflandırma algoritması, Naive Bayes sınıflandırıcısını kullanarak kötü amaçlı yazılımların çeşitli özelliklerini ayıklamak için kullanılır. Önerilen teknik, kötü amaçlı yazılımın algılanma süresini daha hızlı ve doğru şekilde bilmek ve kötü amaçlı yazılım bilgilerini duyurmak için Blok Zinciri teknolojisinde yararlanmaktadır.

## 2. Literatür Araştırması

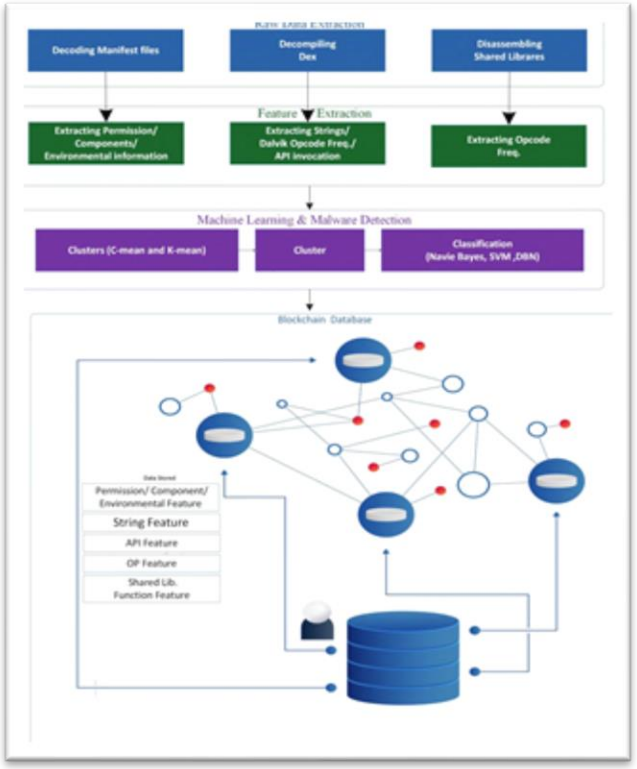
Bu bölümde iki yöntemden oluşan Statik Analiz araştırılmıştır.[3]

1. Statik Analiz
   1.1 İzin Tabanlı Analiz
   1.2 Şüpheli API Çağrıları
2. Dinamik Analiz
3. Hibrit Analiz

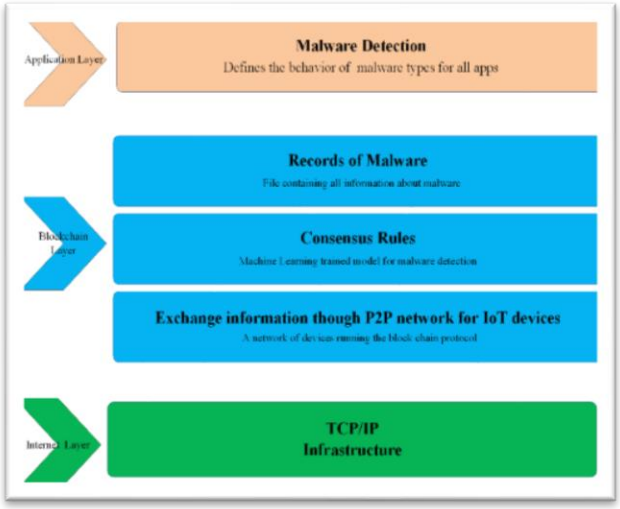
## 3. Veri Seti

Bu makalede, veri seti kötü amaçlı yazılım ve iyi huylu uygulamalardan oluşmaktadır. Veri kümesinde Google Play Store ve Çince Uygulama mağazasından toplanan 6192 iyi huylu ve 5560 kötü amaçlı yazılım uygulaması bulunmaktadır.

## 4. Kullanılan Şema ve Metotlar




Şekil-1 Önerilen Yöntemin Mimarisi




Şekil-2 IoT cihazları için Blok Zinciri tabanlı kötü amaçlı yazılım tespiti.

## 5. Deneysel Sonuçlar

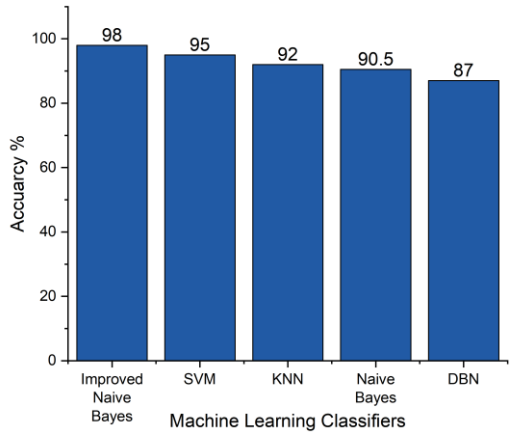
Python programlama dili veri ön işleme, sınıflandırma, kümeleme, regresyon, ilişkilendirme kuralları ve görselleştirme için araçlar içerir, bu da veri bilimcilerinin sınıflandırıcıların performansını ölçmeleri ve test etmeleri için en iyi araçtır. Sınıflandırıcıları değerlendirmek için çeşitli kriterler vardır ve seçilen hedeflere göre kriterler belirlenir. Sınıflandırma yöntemleri için Doğru Pozitif Oran (TPR) ve Yanlış Pozitif Oran (FPR) ve sınıflandırma doğruluğu değerlendirilmektedir. Kötü amaçlı uygulamalar için gerçek pozitiflerin sayısı aşağıdaki formüller:

$$TPR = \frac{T_p}{T_p + F_n} \qquad FPR = \frac{F_p}{F_n + T_n}$$

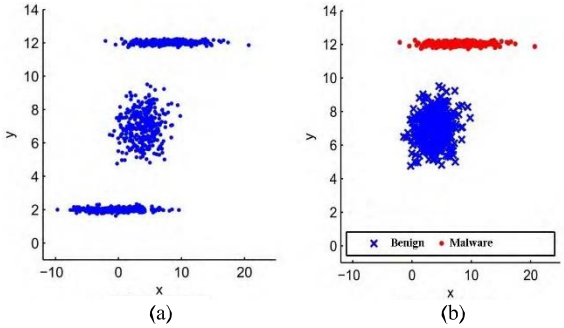
$$Accuracy = \frac{T_p + T_n}{T_p + T_n + F_p + F_n}$$

Yapılan deneylerin sonuçları:

| Alogrthim | TPR | FPR | ACC |
|---|---|---|---|
| Improved Naive Bayes | 98.2 | 98.2 | 98.0 |
| SVM | 95.2 | 95.2 | 95.0 |
| KNN | 75.8 | 87.5 | 92.0 |
| Naive Bayes | 80.5 | 80.7 | 90.5 |
| DBN | 84.6 | 85.0 | 87.0 |




Şekil-3 Sınıflandırıcılarının Başarımı




Şekil-4 İyi ve Kötü Yazılımların Kümelenmesi

Deney sonuçları, önerilen tekniğin çıkarılan özelliklerinin önemini kanıtlamak için yapılmıştır. Yüksek boyutlu ve gürültülü veri kümesi kümeleme algoritmasına göre optimize edilirken, kümeleme sonuçları Şekil-4 de gösterilmiştir. Kümelenmiş verilerde kırmızı renk kötü amaçlı örnekleri gösterir ve mavi renk iyi huylu örnekleri gösterir .

## 6. Sonuç

Bu çalışmada Android IoT cihazlarındaki kötü amaçlı yazılım tespiti için Blok Zinciri ve Makine Öğrenmesi yöntemleri kullanılmıştır. Kötü amaçlı yazılım bilgileri, kümeleme ve sınıflandırma gibi Makine Öğrenmesi teknikleri kullanılarak çıkarılmış ve ayrıca bu bilgiler Blok Zincirinde saklanmıştır. Böylece, Blok Zinciri geçmişinde saklanan tüm kötü amaçlı yazılım bilgileri ağ üzerinden iletilebilir ve bu nedenle kötü amaçlı yazılımlar etkili bir şekilde tespit edilebilir. Önerilen kümeleme yöntemi, her özellik grubunun ağırlıklarını hesaplar ve kötü amaçlı yazılımlar birçok benzer özelliğe sahip olsa da, kötü amaçlı yazılım ve iyi niyetli uygulamaları ayırt etmek için çok etkili olabilecek gereksiz özellikleri yinelemeli olarak azaltır. İkinci olarak, sınıflandırma algoritması, yüksek doğruluk ve sağlamlık elde etmek için çok özellikli sorunları ele alarak bir karar ağacına dayanan Naive Bayes sınıflandırıcısı kullanılarak uygulanır.

## 7. Referanslar

[1] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, ‘‘Blockchain,’’ Bus. Inf. Syst. Eng., vol. 59, no. 3, pp. 183–187, 2017.

[2] V. M. Afonso, M. F. de Amorim, A. R. A. Grégio, G. B. Junquera, and P. L. de Geus, ‘‘Identifying android malware using dynamically obtained features,’’ J. Comput. Virol. Hacking Techn., vol. 11, no. 1, pp. 9–17, Feb. 2015

[3] Y. J. Ham, D. Moon, H. W. Lee, J. D. Lim, and J. N. Kim, ‘‘Android mobile application system call event pattern analysis for determination of malicious attack,’’ Int. J. Secur. Its Appl., vol. 8, no. 1, pp. 231–246, 2014.