SİBER GÜVENLİKTE MAKİNE ÖĞRENMESİ

Ankara Üniversitesi

Bölüm Tanıtımı

- Bu bölümde
  - **Makine öğrenimi, DL (deep learning) ve RL (reinforcement learning) kötü amaçlı yazılım algılama, izinsiz giriş algılama, güvenlik açığı değerlendirme ve diğer alanlardaki kullanımları**
  - **Veri kalitesi, yorumlanabilirlik ve rakip saldırılar da dahil olmak üzere bu tekniklerin zorluklarını ve sınırlamaları**

  ayrıntılı olarak ele alınmıştır.

Giriş

- Hayatımızın her alanında teknoloji bize birçok kolaylık sağlamakla birlikte birçok soruna da yol açmaktadır. Sadece son beş yılda, büyük yıkıcılığa sahip pek çok saldırı oldu. Bu saldırılardan bazıları aşağıda verilmiştir:
  - Equifax Data Breach
  - WannaCry Ransomware Attack
  - Marriott Data Breach
  - Capital One Data Breach
  - SolarWinds Supply Chain Attack
  - Colonial Pipeline Ransomware Attack

Makine Öğrenmesi

- Makine öğrenimi (ML), siber güvenlikte giderek daha popüler bir araç haline geldi.
- Makine öğrenimi, verileri analiz edebilen ve bu verilerle ilgili tahminler yapabilen algoritmalar ve istatistiksel modeller geliştirmeye odaklanan yapay zekanın (AI) bir alt alanıdır.
- Siber güvenlikte makine öğrenimi algoritmaları, tehditlerin varlığına işaret edebilecek kalıpları ve anormallikleri belirlemek üzere eğitim için büyük miktarda veri işler.
- Makine öğrenimi, izinsiz giriş tespiti, kötü amaçlı yazılım tespiti, ağ trafiği analizi ve dolandırıcılık tespiti dahil olmak üzere çeşitli siber güvenlik uygulamalarında kullanılabilir.

Makine Öğrenmesi Avantajları

- Siber güvenlikte makine öğrenimi kullanmanın birkaç önemli avantajı vardır:
- **Geliştirilmiş doğruluk:** Makine öğrenimi algoritmaları, büyük miktarda veriyi analiz edebilir ve insan analistlerin algılaması zor olabilecek kalıpları belirleyebilir. Bu, daha yüksek oranda doğru tehdit tespiti ve daha az yanlış pozitif ile sonuçlanabilir.
- **Daha hızlı tespit:** ML algoritmaları, verileri gerçek zamanlı olarak analiz ederek potansiyel tehditlerin daha hızlı tespit edilmesini ve bunlara yanıt verilmesini sağlar.
- **Otomasyon:** ML algoritmaları, insan analistlerin daha karmaşık görevlere odaklanmasına izin vererek, tehdit algılama ve yanıt vermeyle ilişkili birçok zaman alan görevi otomatikleştirir.
- **Ölçeklenebilirlik:** Makine öğrenimi algoritmaları, büyük miktarda veriyi analiz edecek şekilde ölçeklenebilir ve bu da onları büyük ölçekli siber güvenlik operasyonları için çok uygun hale getirir.

Makine Öğrenmesi Sınırları

- Makine öğreniminin siber güvenlik için birçok faydası olsa da her saldırıyı tespit etmek için kesin çözüm değildir. Dikkate alınması gereken birkaç sınırlama vardır:
- **Veri kalitesi:** Makine öğrenimi algoritmaları, yüksek kaliteli verilerle verimli bir şekilde çalışır. Algoritmaları eğitmek için kullanılan veriler eksik veya yanlışsa, yanlış tahminlere yol açabilir.
- **Karmaşıklık:** Makine öğrenimi algoritmaları karmaşık ve yorumlanması zor olabilir, bu da insan analistlerin algoritmaların nasıl karar verdiğini anlamalarını zorlaştırır.
- **Düşmanca saldırılar:** Makine öğrenimi algoritmaları, bir saldırganın algoritma tarafından tespit edilmekten kaçınmak için kasıtlı olarak verileri manipüle ettiği düşmanca saldırılara karşı savunmasız olabilir.

Makine Öğrenmesi Uygulama Alanları

- **İzinsiz Giriş Tespiti:** Makine öğrenimi algoritmaları, ağ trafiğini izleyebilir ve bir siber tehdidin varlığını gösterebilecek olağandışı kalıpları algılayabilir. Örneğin, anormallik algılama algoritmaları, bir Dağıtılmış Hizmet Reddi (DDoS) saldırısına işaret edebilecek olağandışı ağ trafiği kalıplarını algılayabilir.
- **Kötü Amaçlı Yazılım Tespiti:** Makine öğrenimi algoritmaları, kötü amaçlı yazılımları davranışlarını veya özelliklerini göz önünde bulundurarak tanımlayabilir ve sınıflandırabilir. Örneğin, denetimli bir öğrenme algoritması, bilinen veri kümesiyle benzerliklerine dayalı olarak yeni kötü amaçlı yazılım örneklerini belirlemek için bilinen bir kötü amaçlı yazılım veri kümesi üzerinde eğitilir.
- **Dolandırıcılık Tespiti:** Makine öğrenimi algoritmaları, finansal işlemlerdeki hileli faaliyetleri de tespit edebilir. Örneğin, bir dolandırıcılık algılama algoritması, dolandırıcılığa işaret edebilecek olağandışı kalıpları belirlemek için işlem verilerini analiz edebilir.

Makine Öğrenmesi Uygulama Alanları

- **İstenmeyen Posta Algılama:** Makine öğrenimi, iletilerin içeriğini ve özelliklerini analiz ederek istenmeyen e-postaları filtrelemek için kullanılabilir.
- **Tahmine Dayalı Analitik:** Makine öğrenimi, geçmiş verileri analiz ederek ve potansiyel bir tehdide işaret edebilecek kalıpları belirleyerek gelecekteki siber saldırıları tahmin etmek için kullanılabilir.
- **Güvenlik Açığı Yönetimi:** Makine öğrenimi, en kritik riskleri belirlemek için güvenlik açığı tarayıcıları ve ağ trafiği gibi birden çok kaynaktan gelen verileri analiz ederek güvenlik açıklarına öncelik vermek için kullanılabilir.
- **Tehdit İstihbaratı:** Ortaya çıkan tehditleri ve güvenlik açıklarını belirlemek için birden çok kaynaktan gelen tehdit istihbaratı verilerini analiz etmek için makine öğrenimi kullanılabilir.

Derin Öğrenme

- Derin öğrenme (DL), verilerdeki karmaşık kalıpları ve ilişkileri otomatik olarak öğrenme yeteneği nedeniyle popülerlik kazanan makine öğreniminin bir alt alanıdır.
- Doğal dil işleme, bilgisayar görüşü ve konuşma tanıma gibi birçok alanda umut verici sonuçlar vermiştir.
- Ayrıca siber güvenlik konusunda da çok yüksek bir potansiyel gözlemlemiştir.
- Derin öğrenme, siber güvenliğe çeşitli şekillerde yardımcı olabilir:
  - Kötü amaçlı yazılım tespiti
  - Saldırı tespit sistemleri
  - Dolandırıcılık tespiti

Derin Öğrenme Uygulama Alanları

- **Kötü amaçlı yazılım tespiti**, siber güvenlikte derin öğrenmenin en umut verici uygulamalarından biridir. Kötü amaçlı yazılımları tespit etmenin geleneksel yöntemleri, yazılım imzalarından oluşan bir veritabanıyla karşılaştırmayı içeren imza tabanlı algılamaya dayanır. Ancak bu yöntem etkisizdir çünkü saldırganlar tespit edilmekten kaçınmak için kodlarını kolaylıkla değiştirebilirler. Derin öğrenme, davranışsal algılama olarak bilinen kodu yerine programın davranışını analiz ederek kötü amaçlı yazılımları algılamak için kullanılabilir.
- Geleneksel **IDS sistemleri**, şüpheli veya kötü amaçlı etkinlik türlerini tanımlayan kurallar yazmayı içeren kural tabanlı algılamaya dayanır. Derin öğrenme bunun yerine, ağ trafiğini analiz ederek ve bir saldırının göstergesi olan kalıpları belirleyerek izinsiz giriş tespitini iyileştirmek için kullanılabilir.

Derin Öğrenme Uygulama Alanları

- Dolandırıcılık, bankacılık, sigortacılık ve e-ticaret dahil olmak üzere birçok sektörde önemli bir sorundur. **Geleneksel dolandırıcılık tespit** yöntemleri, bilinen dolandırıcılık kalıplarını belirlemek için kural tabanlı sistemlere dayanır. Derin öğrenme, işlemlerin büyük veri kümelerini analiz ederek ve dolandırıcılık faaliyetinin göstergesi olan kalıpları belirleyerek dolandırıcılığı tespit etmek için kullanılabilir. Eğitimli DL algoritmaları bu kalıpları algılayabilir ve şüpheli işlemleri işaretleyebilir.
- Özetle, derin öğrenme, siber saldırıları tespit etmek ve önlemek için yeni bir dizi araç sağlayarak siber güvenlikte ilerleme potansiyeline sahiptir.

Takviyeli (Reinforcement) Öğrenme

- Takviyeli Öğrenme (RL), bir aracının bir dizi deneme yanılma deneyimi yoluyla bir ortamla nasıl etkileşim kuracağını öğrenmesini içeren bir makine öğrenimi alt alanıdır.
- Temel fikir, simüle edilmiş bir ortamla etkileşime giren bir aracıyı eğitmek ve gerçek zamanlı olarak potansiyel güvenlik tehditlerini nasıl belirleyeceğini ve bunlara nasıl tepki vereceğini öğrenmektir.
- Siber güvenlikte, yeni tehditlere uyum sağlamak, RL'nin en önemli faydalarından biridir. RL aracıları, ortamdaki deneyimlerine dayalı olarak sürekli öğreniyor ve gelişiyor.
- RL'nin siber güvenlikteki diğer bir avantajı, geri bildirimden öğrenme gücüdür. RL aracıları, ortamdaki eylemlerine göre ödüller veya cezalar alır. Bu geri bildirim, hangi eylemlerin olumlu sonuçlara yol açma olasılığının daha yüksek olduğunu ve hangi eylemlerden kaçınılması gerektiğini öğrenmelerini sağlar.

Takviyeli Öğrenme Uygulama Alanları

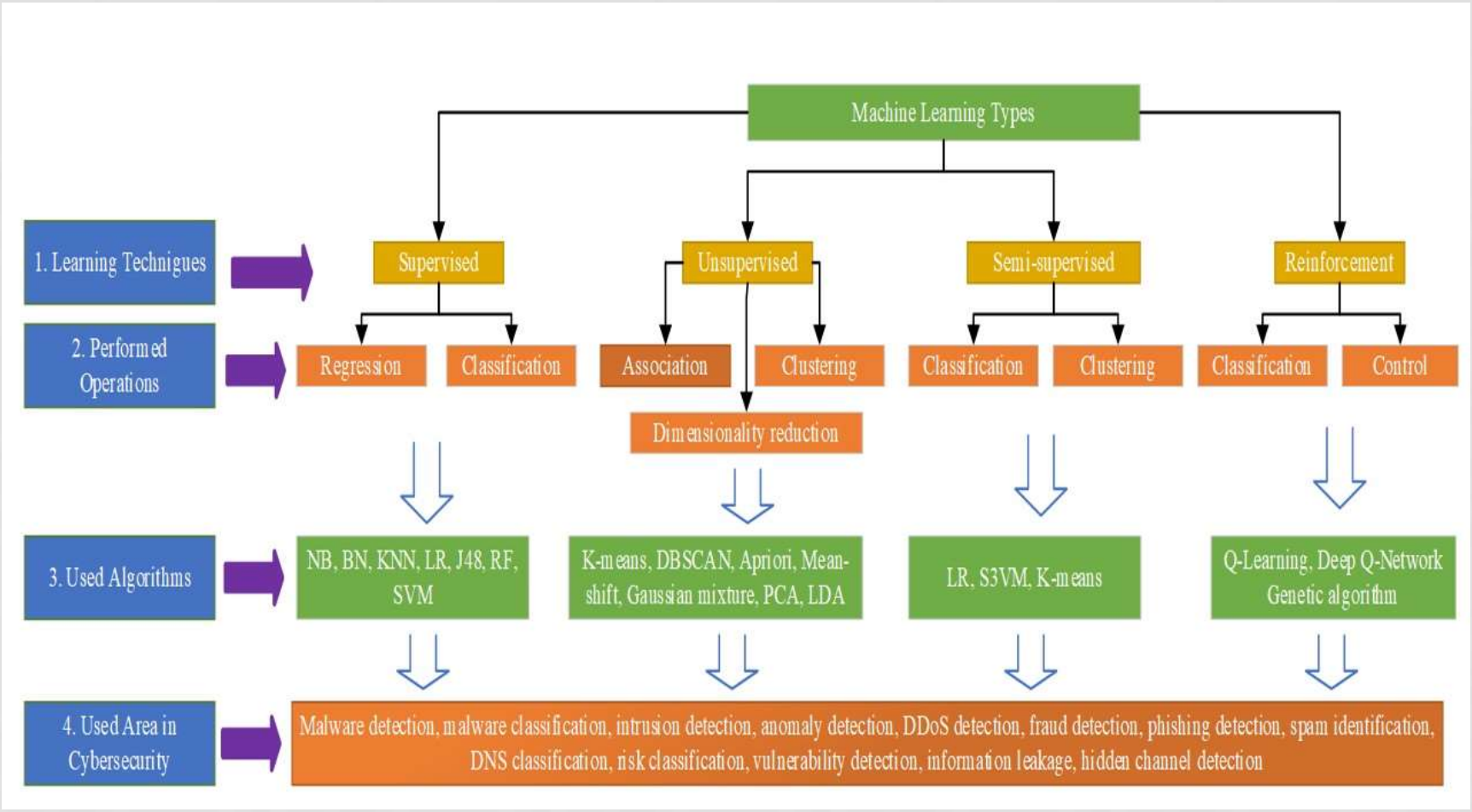
- Ağ trafiğini gözlemlemek ve şüpheli etkinliği gerçek zamanlı olarak tespit etmek.
- Daha etkili parola politikaları geliştirmek.
- IoT cihazlarının güvenliğini artırmak
- Güvenlik açığı yönetimi
- Siber tehdit istihbaratı

Özetle, RL, yeni ve gelişmekte olan tehditleri hızlı bir şekilde tanımlayabilen ve bunlara yanıt verebilen daha dinamik ve uyarlanabilir güvenlik sistemleri sağlayarak siber güvenlikte ilerleme kaydetme potansiyeline sahiptir.

Makine Öğrenmesi Siber Güvenlikte Neden Popüler?

- ML, veri ihlallerinin, güvenlik açıklarının, kötü amaçlı yazılımların ve diğer ilgili sorunların manuel müdahale olmaksızın otomatik olarak tespit edilmesini sağlayarak siber güvenlik sektörü için dikkate değer bir değişiklik sağlamıştır.
- ML, büyük miktarda veriyi analiz etmenin daha hızlı bir yolunu sağladı.
- ML, ayarlamalar için uzman girişi gerekliliğini ortadan kaldırdı.
- ML, gereksiz alanı önemli ölçüde azalttı, bu da onu güçlü ve etkili bir yöntem haline getiriyor.
- ML, tehdit algılama doğruluğunu artıran ve ağ güvenliğini artıran yeni yöntemler oluşturmak için geliştirildi.
- ML, buluşsal yöntemler ve budama teknikleri kullanan etkili arama yöntemlerine sahiptir.

Makine Öğrenmesi Teknikleri



1.Denetimli ML

- İşlem sırasında geliştirici denetimi gerektiren algoritmalar, denetimli makine öğrenimi olarak bilinir. Geliştirici, eğitim verilerini etiketler ve algoritmanın izleyeceği katı kuralları ve sınırları belirler.
- Denetimli yaklaşımın amacı, bir dizi girdi üzerinde kurulan bir işlevi kullanarak hedef değişkeni tahmin etmektir.
- Bir algoritma, çıktısını doğru sonuçla karşılaştırarak ve hataları belirleyerek de kendini değiştirebilir.
- Denetimli ML tekniği, daha önce görülen benzer siber saldırıları tespit etmek için uygundur.
- Denetimli makine öğrenimi tekniği temel olarak siber güvenlikte kötü amaçlı yazılım tespiti, spam tespiti, anormallik tespiti ve risk puanlaması için kullanılır.

2.Denetimsiz ML

- Denetimsiz makine öğrenimi yöntemleri, eğitim verilerinde etiketleme veya kategorileştirme olmadığında kullanılır.
- Sistemin çıktıyı doğru tanımlayamadığını varsayalım. Bu durumda, etiketlenmemiş verilerdeki gizli yapıları aydınlatmak için verileri incelemeye ve veri kümelerinden içgörüler çıkarmaya devam eder.
- Denetimsiz teknik, sistemdeki anormallikleri belirlediği için bilinmeyen saldırıların türlerini de belirleyebilir.
- Denetimsiz makine öğrenimi tekniği genellikle siber güvenlikte anomali tespiti, IoT tabanlı sıfır gün saldırıları, varlık sınıflandırması ve veri keşfi için kullanılır.

3. Yarı Denetimli ML

- Denetimli ve denetimsiz algoritmaların kombinasyonlarına yarı denetimli makine öğrenimi denir.
- Sürecin başında etiketlenmemiş veriler ve eksik kurallar olabilir.
- Yarı denetimli teknik, sistemde yeni siber saldırılar meydana geldiğinde anormallikleri tanımlayabilir ve ardından bu anormallikleri diğer siber saldırı türlerini verimli bir şekilde tespit etmek için kullanabilir.
- Ağdaki izinsiz girişleri, DDoS saldırılarını ve kötü amaçlı yazılım saldırılarını tespit etmek için kullanılabilir.

4. Takviyeli

- Bu tür algoritmalarda, bir ajanın çevresiyle etkileşime girerek eylemler ürettiği, sonuçları gözlemlediği, ardından bir sonraki eylemi gerçekleştirirken bu sonuçları dikkate aldığı ve algoritma gelişene ve doğru stratejiyi seçene kadar bu şekilde devam ettiği keşif adı verilen bir teknik kullanılır.
- Makineler ve yazılım aracıları tarafından kullanılan bu teknik, performanslarını en üst düzeye çıkarmak için belirli bir durumda en iyi eylem setini otomatik olarak belirlemelerini sağlar.
- RL, sistem üzerinde sızma testleri, risk değerlendirmesi ve anormal davranışlar gerçekleştirmek için kullanılabilir.

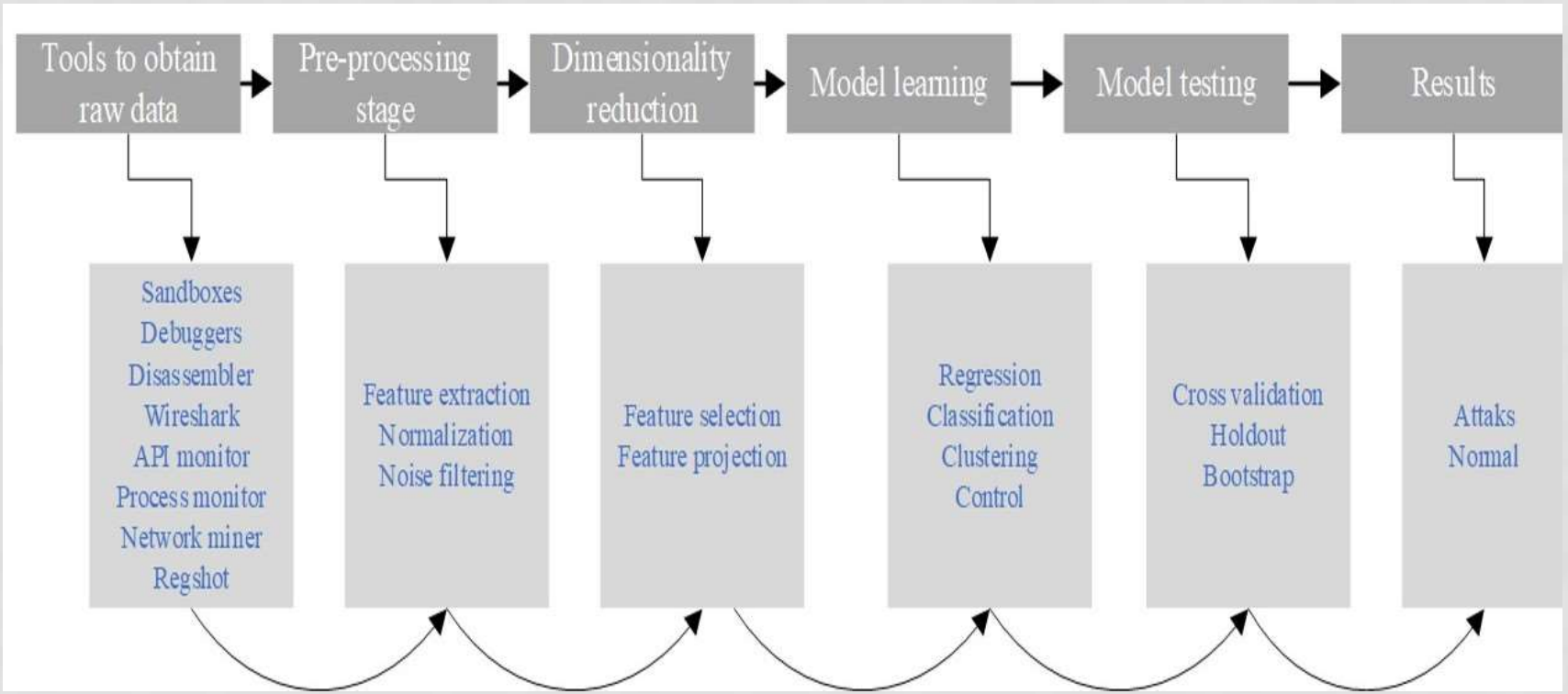
Makine Öğrenmesi Algoritmaları

- Makine öğrenimi, siber güvenlikte çeşitli amaçlar için kullanılabilen çok çeşitli algoritmaları kapsar. Bu algoritmalar kullanılarak regresyon, sınıflandırma, kümeleme, boyut azaltma ve artırma işlemleri gerçekleştirilebilir.
  1. Regression
  2. Probabilistic
  3. Distance based
  4. Decision tree
  5. SVM
  6. Dimensionality reduction
  7. Boosting and Bagging

Makine Öğrenmesi Algoritmaları

Algorithm	Classifiers	Pros	Cons
Decision Trees	RF, ID3, CART, C4.5, LMT, J48	İşlemleri hızlı gerçekleştiren, ölçeklenebilir mantık tabanlı algoritmalar.	Algoritma çıktılarının analiz edilmesi zordur ve sürekli sınıf değerlerini tahmin etmede etkili değildir.
Probabilistic	Naïve Bayes, Bayes Networks	Hızlı çalışma, çok sınıflı tahminleri etkili bir şekilde hesaplama ve yüksek boyutlu verilerde iyi performans gösterme	Aşırı özellik sayısına sahip veri kümeleri için etkili değildir.
Distance Based	KNN, K-Mean, LVQ	Veriler hakkında bilgi olmadığında iyi çalışır.	Zaman ve depolama maliyeti yüksektir ve performans kullanılan parametrelere bağlıdır.
SVM	Linear, Nonlinear, SMO, different kernels	Yüksek boyutlu verilerde iyi performans gösterir ve sınıflar ayrılabilirolduğunda başarılı olur.	Çakışan sınıflarda iyi performans gösteremez ve uygun çekirdek işlevini seçmek zor olabilir.
Regression	SLR, Linear, Logistic	Basit ve etkili performans gösteren tahmine dayalı algoritma.	Doğrusal olmayan veriler için performans zayıftır.
Boosting and Bagging Algorithms	AdaBoost, LightGBM, XGBoost	Modelin doğruluğunu artırır ve overfittingi azaltırken varyansı azaltmaya da yardımcı olur.	Gerçek zamanlı olarak uygulanması zordur ve yüksek yanlılığa neden olarak kötü uyumla sonuçlanabilir.
Dimensionality Reduction Algorithms	PCA, LDA, GDA	Hesaplama süresini azaltır ve algılama doğruluğunu artırır.	Daha düşük performansla sonuçlanan veri kaybına neden olabilir.

Veri Toplamadan Sonuçlara Kadar Makine Öğrenme Süreçleri



Siber Güvenlik Alanında Makine Öğrenimindeki Önemli Zorluklar

- Veriler hakkında varsayımlarda bulunmak
- Akışlarda yeterli bilgi olmaması, bağlamsal özelliklere ihtiyaç duyar
- Aşırı miktarda veri
- Yüksek boyutluluk
- Çok sayıda veri mevcuttur, ancak tek bir kayıt iyi veya kötü olduğunu göstermez
- Verilere önyargılı yaklaşım nedeniyle anlamlı özellikler tasarlamak zor (ör. ikili dosyalar için bayt akışı)
- Veri ön işleme zorlu bir iştir
- Özellik mühendisliği, parametre seçimleri vb. gibi sürecin çeşitli bölümleri, algoritmanın performansı adına çok önemlidir.
- Alan bilgisi dikkate alınmaz
- Aykırı değerler kontrol edilemez
- Bilinmeyen saldırılardan gelen verileri tespit etmek ve önlemek zor
- Saldırıların üstesinden gelinmesi daha karmaşık hale gelir ve makine öğrenimi algoritmalarından kaçılmasına neden olur.

Özet

- ML, DL ve RL, siber güvenliği iyileştirmek için hayati araçlar haline geliyor. Bu yaklaşımlar, kötü amaçlı yazılım, kimlik avı ve hizmet reddi saldırıları dahil olmak üzere çok çeşitli siber saldırıları belirleme ve bunlara karşı savunma yapma becerisini göstermiştir.
- Büyük veri kümelerinden ve güçlü algoritmalardan yararlanan bu teknikler, kuruluşların sürekli gelişen tehditlerin önünde kalmasına yardımcı olabilir.
- Makine öğrenimi ve DL'nin siber güvenlik bağlamında kullanımıyla ilgili, yüksek kaliteli verilere duyulan ihtiyaç ve yanlış pozitif potansiyeli gibi kesinlikle zorluklar olsa da, potansiyel faydalar önemlidir.
- Bu teknolojilerin devam eden gelişimi ve mevcut çözümlere entegre edilmesi, önümüzdeki yıllarda daha etkili savunma mekanizmaları oluşturması daha olasıdır.

Özet

- Makine öğrenimi, siber güvenliği iyileştirmek için kullanılabilecek güçlü bir araçtır.
- Makine öğrenimi algoritmaları, büyük veri kümelerini analiz ederek ve ağ etkinliğindeki kalıpları belirleyerek kuruluşların potansiyel tehditleri gerçek zamanlı olarak algılamasına ve bunlara yanıt vermesine yardımcı olabilir. Bu, bir kuruluşun genel güvenlik duruşunu iyileştirmenin yanı sıra siber saldırılara daha hızlı ve daha etkili yanıtlar verebilir.
- Teknoloji gelişmeye ve daha karmaşık hale gelmeye devam ettikçe, gelecekte muhtemelen daha da etkili savunma mekanizmaları göreceğiz. Siber güvenlikte makine öğreniminin potansiyelini tam olarak gerçekleştirmek için kuruluşların araştırma ve geliştirmeye yatırım yapması ve uygulamayla ilgili zorlukları ele almak için çalışması çok önemlidir.