**Anomaly Detection using Machine Learning Techniques**

Özet— Makine öğrenimi algoritmaları, sistemlerin davranışı gerçek verilere dayalı olarak gözlemlemesini sağlar. Geçmiş deneyimlere dayalı olarak, bilgisayarların geçmiş deneyimlerden öğrenilen davranışları sergilemesine izin veren algoritmalar tasarlanabilir. Makine öğrenimi algoritmaları, belirli bir ağdaki anormal örnekleri analiz etmek için kullanılır. Algoritmalar birden çok veri için eğitilebilir ve bir ağdan yararlanmayı izleyebilir. Bu fikir dolandırıcılık tespiti ve makinelerin izlenmesi için kullanılır. Denetimli öğrenme, bir ağdaki anormal davranışın eğitimi ve analizi açısından çok önemlidir. Bu makale, ağ anormalliklerini tespit etmek için kullanılan denetimli teknikleri sunmaktadır.

I. INTRODUCTION

Anormallik tespiti, aykırı değerler olarak adlandırılan beklenmedik kalıpları belirlemede kullanışlıdır. Ağ trafiğindeki, sistem sağlığı izlemesine bir saldırı olabilecek (MRI taramasında kötü huylu bir tümörü tespit etme) garip kalıpları tanımlar. Makine öğrenimi algoritmaları, geçmiş saldırıları analiz etmek ve uygun savunma yanıtları geliştirmek için kullanılır [1].

Algoritmalar, belirli bir kaynağın veya web sitesinin dizin geçişlerini analiz eder ve web uygulama hizmetlerinin güvenlik standartlarını sağlar. Hedef yolu üzerinden yönlendirilen kötü amaçlı web siteleri de tespit edilir [1,2].

Yol geçişlerini tespit etmeye yönelik algoritmalar, çeşitli kötü amaçlı etki alanlarını belirlemek için kullanılabilir. Bu algoritmalar ayrıca bir ana bilgisayardan gelen anormal kalıpları da algılayabilir. Sinir ağları, bilinmeyen kötü amaçlı saldırıları tespit etmek için kullanışlıdır. Veri kümeleri, kötü amaçlı veya fidye dosyalarının davranışını analiz etmek için uygun şekilde eğitilmiştir. Eğitim süreci için çok sayıda fidye dosyası ve temiz dosya gereklidir.

Algoritmalar, veri kümesindeki her dosyanın temel özelliklerini tanımlamak için kullanılır. Özellikler, elde edilen veri seti için modeli eğitmek üzere alt kümelere ayrılmıştır. Bir sistem virüslü bir dosya tarafından saldırıya uğradığında, bu dosya eğitimli model tarafından kontrol edilir ve tüm dosya sistemi şifrelenmeden veya bilgisayara erişimi kilitlemeden önce önlemler alınır.

Uzaktan istismar olarak da bilinen uzaktan saldırı, birkaç bilgisayar ağının saldırıya uğradığı bir saldırıdır. Sisteme saldırgan tarafından güvenlik açığı noktalarından erişilir. Bu tür bir saldırının hedefi, sistemden hassas verilerin kullanılması ve çalınmasıdır. Uzaktan saldırılar aşağıdaki şekillerde mümkündür:

* Hizmet Reddi saldırısı: Sunucuyu kullanıcı tarafından kullanılamaz hale getirmek için sunucular büyük miktarda yanlış istemci istekleriyle dolar. Sunucu, büyük miktarda bekleyen müşteri istekleriyle dolup taşıyor [14].
* DNS zehirlenmesi: facebook.com gibi alan adları bazı sayısal IP adreslerine çevrilir. DNS zehirlenmesinde, sunucular temel olarak yanlış veri kaynaklarını meşru olarak kabul etmeleri için kandırılır ve zehirlenen DNS sunucularına erişen kullanıcılar, virüsleri sisteme indiren virüslü sitelere yönlendirilir.
* Port tarama: Bir ağdaki açık portlar, bir port tarayıcı kullanılarak tanımlanır. Veriler bilgisayar portları aracılığıyla gönderilir ve alınır. Böylece olası güvenlik açıkları da tespit edilir. Saldırgan, ağa erişim sağlayarak güvenlik açığından yararlanır.

Bir sistemdeki tipik ağ davranışıyla ilişkili olmayan anormal durumlar, makine öğrenimi algoritmaları tarafından belirlenebilir ve analiz edilebilir. İstismar yükünü izlemek için birden çok veri kümesi için eğitim yapılabilir. Verilerden öğrenmek ve tahminler yapmak için algoritmaları kullanan otomasyona makine öğreniminde izin verilir. Algoritmalar denetimli veya denetimsiz olabilir. Denetimsiz öğrenmede sistem, güncellenen verilere göre otomatik olarak öğrenir.

II. ANOMALY DETECTION

Aykırı değerler olarak adlandırılan bir ağdaki anormal kalıpları tanımlayan bir mekanizmadır.

Garip modelin ağ trafiğini belirlemede kullanışlıdır. Anormallikler genel olarak şu şekilde sınıflandırılır:

**Nokta Anomalileri**: Veri noktasının değeri, bulunduğu veri setinin tamamının çok dışındadır.

**Bağlamsal Anomaliler**: Zaman serisi verilerinde yaygındır. Anormal davranış bağlama özgüdür.

**Kolektif anormallikler**: Veri örnekleri, anormalliklerin tespitinde kullanılır. Algoritmayı oluşturma adımları şunlardır:

1. Anormal verilerin x özellikleri çıkarılır

2. μ ve σ parametreleri hesaplanır

3. x'in p olasılığı hesaplanır

4. Belirlenen olasılık sınırı ϵ test edilir

Bir Gauss dağıtım algoritması kullanılarak, örnek x aşağıdaki gibi dağıtılır: