1. LinkedIn Paylaşım Önerisi (Detaylı Versiyon)

Başlık: Elektrikli Araç (EV) Şarj Altyapılarında Veri Manipülasyonu ve Gelir Kaybı Riski

Şarj istasyonu güvenliği projemiz kapsamında, literatürde de yer alan **"Adaptif Örnekleme Manipülasyonu"** (Sampling Manipulation) üzerine derinlemesine bir çalışma gerçekleştirdik.

+1

🔍 **Saldırı Mekanizması Nasıl İşliyor?** Geleneksel enerji hırsızlığından farklı olarak bu yöntem, cihazın örnekleme hızını (sampling rate) hedef alır. Normal şartlarda saniyelik alınan veriler, saldırgan tarafından kasıtlı olarak seyreltilir (örneğin 60 saniyeye bir). Bu durum, anlık yüksek güç çekişlerinin (peak points) ortalamaya gömülerek "görünmez" hale gelmesine neden olur.

+3

🛡️ **Geliştirdiğimiz Tespit Stratejisi:** Statik kurallar yerine, verinin karakteristiğini analiz eden 3 aşamalı bir kontrol mekanizması kurguladı:

- **Örnekleme Hızı Denetimi:** Beklenen minimum veri akış hızının altına düşüldüğünde anında alarm üretilir.
- **Varyans ve Enerji Düzlüğü Analizi:** Güç profilindeki dalgalanma miktarı (variance) geçmiş verilere göre %30'dan fazla azaldığında, peak değerlerin gizlendiği tespit edilir.
- **Tampon Bellek (Buffer) Tutarsızlığı:** Yerelde biriken ham veri ile sunucuya gönderilen özet veri arasındaki uçurum, manipülasyonun kanıtı olarak sunulur.

📊 **Sonuçlar:** Simülasyon testlerimizde **%95 tespit oranı** ve **10 saniyenin altında alarm süresi** ile manipülasyonu yakalamayı başardık.

Siber güvenliği sadece veri gizliliği olarak değil, enerji ekonomisinin ve şebeke kararlılığının teminatı olarak görüyoruz.

#CyberSecurity #EVCharging #SmartGrid #AnomalyDetection #EnergyEfficiency #DataIntegrity

Görsel Önerisi:

- **İnfografik Tarzı:** Ekranın solunda "Normal Akış" (Sık veri noktaları ve yüksek iniş çıkışlar), sağında "Saldırı Anı" (Seyrek veri noktaları ve düzleşmiş bir grafik) olan bir karşılaştırma görseli.

Dashboard Görünümü: Geliştirdiğin "Kural-1: Sampling Düşüşü" uyarısının yandığı kırmızı bir alarm ekranı görseli