Literatür Karşılaştırması: SWOT Analizi

Makale Adı: ML-FEED: Machine Learning Framework for Efficient Exploit Detection

Proje Adı: Yapay Zekâ Tabanlı Faturalandırma Sistemlerinde Gecikme (Latency) Kaynaklı Zafiyet

Bu analiz, "ML-FEED" başlıklı çalışmanın, mevcut projemizin teorik altyapısı ve özgün katkısı bağlamında sunduğu güçlü yönleri, zayıflıkları, fırsatları ve tehditleri değerlendirmektedir.

1. Güçlü Yönler (Strengths)

(Makalenin, projemizin varsayımlarını destekleyen yönleri)

- **Kök Neden Doğrulaması:** Makale, projemizin temel aldığı "Al Gecikmesi" varsayımını güçlü bir şekilde doğrulamaktadır. Çalışma, LSTM ve Transformer gibi modern YZ modellerinin "ciddi hesaplama yükü (gecikme)" (significant computation overheads) getirdiğini açıkça belirtmektedir.
- **Problem Alanı Teyidi:** Makale, bu yüksek gecikmenin, YZ modellerinin "gerçek zamanlı ortamlarda" (real-time environments) kullanılmasını "imkansız" (infeasible) hale getirdiğini savunmaktadır. Bu, projemizin "birkaç yüz milisaniye ile birkaç saniye arasında değişebilen karar süresi" tezini ve bunun gerçek zamanlı faturalandırma için yarattığı riski doğrudan desteklemektedir.

2. Zayıf Yönler (Weaknesses)

(Makalenin, projemizin kapsamı dışında kalan veya değinmediği yönleri)

- **Odak Farklılığı:** Makalenin ana amacı gecikmeyi *azaltarak* daha verimli bir saldırı tespit (exploit detection) modeli (ML-FEED) sunmaktır. Oysa bizim projemiz, gecikmeyi azaltmak yerine, mevcut gecikmeyi bir *saldırı vektörü* olarak istismar etmeye odaklanmaktadır.

- **Alan Spesifik Değil:** Çalışma, genel API çağrı dizilerini incelerken, projemiz spesifik olarak OCPP protokolü ve CSMS faturalandırma mantığı üzerine yoğunlaşmıştır.
- **Finansal Boyut Eksikliği:** Makale, gecikmeyi teknik bir performans ve güvenlik tespiti sorunu olarak ele alır; projemizde olduğu gibi bunun "fatura atlama" veya "eksik tahsilat" gibi doğrudan finansal sonuçlarını analiz etmez.

3. Fırsatlar (Opportunities)

(Makalenin bıraktığı ve projemizin doldurduğu araştırma boşlukları)

- **Araştırma Boşluğu (Research Gap):** Makalenin gecikmeyi bir "performans sorunu" olarak tanımlaması, projemizin en büyük fırsatıdır. Projemiz, bu performans sorununu bir **güvenlik zafiyeti** ve **aktif bir istismar yüzeyi** olarak yeniden tanımlayarak literatürdeki bu boşluğu doldurmaktadır.
- **Özgün Katkı:** ML-FEED, "gecikme yüzünden saldırıları kaçırıyoruz" derken; projemiz, "saldırganlar tam da bu gecikmeyi bildikleri için, geçerli mesajlarla sistemi bilinçli olarak manipüle ediyor" diyerek özgün bir "zamanlama manipülasyonu" senaryosu sunmaktadır.
- **Pratik Uygulama:** Makale teorik bir zorluktan bahsederken, projemiz bu teorik sorunun OCPP gibi yaygın bir endüstri standardında nasıl pratik ve finansal bir anomaliye yol açtığını bir simülasyon ile gösterme fırsatı sunar.

4. Tehditler (Threats)

(Makalenin, projemizin özgünlük iddiasını zayıflatabilecek yönleri)

- **Yenilik İddiası:** Makalenin, YZ gecikmesinin gerçek zamanlı güvenlik tespitindeki zorluklarını zaten vurgulamış olması, projemizin "bu yeni bir saldırı yüzeyidir" iddiasının "tamamen yeni" olma niteliğini bir miktar zayıflatabilir.
- **Çözüm Çakışması:** Makalenin önerdiği "ML-FEED" gibi "hafif" (lightweight) modeller, bizim projemizin "Savunma Stratejileri" bölümündeki "Hızlı Ön-Filtreler" (Lightweight Heuristics) önerisiyle kavramsal olarak benzerlik taşımaktadır. Bu durum, projemizin önerdiği çözümlerin özgünlüğünü desteklemek için daha detaylı bir ayrım yapılmasını gerektirebilir.