SWOT ANALİZİ

S – Strengths (Güçlü Yönler)

1. **Kapsamlı literatür taraması**
   - Makale, smart-meter (akıllı sayaç) gizliliği ile ilgili üç temel yöntemi sistematik olarak açıklıyor:
     ✓ Veri manipülasyonu (aggregation, binning, down-sampling, differential privacy)
     ✓ Demand shaping (yük kaydırma)
     ✓ Load scheduling (batarya, yenilenebilir kaynaklarla tüketim maskeleme)
2. **Çok disiplinli yaklaşım**
   - Kriptografi (homomorphic encryption, secret sharing)
   - İstatistik ve bilgi teorisi (mutual information, Fisher information, hypothesis testing)
   - Kontrol/optimizasyon (batarya yönetimi, HVAC kontrolü)
3. **Akademik derinlik + pratik örnekler**
   - Yalnızca teoriyi değil, gerçek veri setleri ve gerçek dünyadaki gizlilik problemleriyle ilişkilendiriyor (örn. Hollanda kanunları, ABD mahkeme kararı).
4. **Yöntemleri kıyaslayan nadir çalışmalar**
   - Tek bir yöntemi anlatmıyor; her yöntemin avantaj/dezavantaj/uygulanabilirlik boyutlarını kıyaslıyor.
5. **Açık erişim olması**
   - Kaynağa herkes ücretsiz ulaşabiliyor → araştırma geniş kitleye yayılabiliyor.

W – Weaknesses (Zayıf Yönler)

1. **Tamamen teorik ve model ağırlıklı**
   - Smart-meter saldırıları **gerçek donanım üzerinde** test edilmiyor.
   - Özellikle batarya/HVAC optimizasyonunun gerçek cihaz kısıtları makalede basitleştirilmiş.
2. **Performans / maliyet analizi sınırlı**
   - Batarya ömrü, maliyet analizi, ROI (return on investment) gibi pratik kısıtlar yeterince ele alınmamış.
3. **Şarj istasyonları / OCPP özelinde değil**
   - Makale konut tipi smart meter gizliliği üzerine; EV şarj istasyonları ve sampling manipulation tekniği doğrudan işlenmiyor.
4. **Bazı öneriler henüz olgun değil**
   - Homomorphic encryption teorik olarak güçlü ancak yüksek CPU/memory maliyeti pratikte engel.

O – Opportunities (Fırsatlar)

Bu çalışma, özellikle *senin raporunla bağlantılı olarak çok fırsat sunuyor.*

1. **Şarj istasyonları için veri manipülasyonu tespit sistemi geliştirme**
    - Makaledeki “down-sampling, aggregation, binning” tanımları → senin senaryondaki "sampling rate düşürme manipülasyonu" ile birebir örtüşüyor.
2. **Anomaly/Intrusion detection (IDS) yaklaşımı katma**
    - Makale manipülasyonu anlatıyor, sen ise "tespit" kısmını yapıyorsun → literatürde açık alan.
3. **Diferansiyel gizlilik → şarj istasyonlarında billing güvenliği**
    - Faturalamada yanlış ücretlendirme / enerji kaybı → EV tarafında yeni kullanım senaryosu.
4. **Batarya kullanımı + gizlilik optimizasyonu**
    - Elektrikli araç bataryaları zaten var → gizlilik ve maliyet optimizasyonu için yeni araştırma alanı.
5. **Regülasyon ve veri gizliliği (KVKK, GDPR) entegrasyonu**
    - Makale mahkeme kararlarından bahsediyor → hukuki dayanaklar yüksek.

T – Threats (Tehditler / Riskler)

1. **Manipülasyon kötüye kullanılabilir**
    - Veri gizleme amacıyla kullanılan teknikler (aggregation, binning, down-sampling)
      → kötü aktörler tarafından **fatura kaçakçılığı/enerji hırsızlığı** için suistimal edilebilir.
2. **Operasyonel risk**
    - Şebeke koruma sistemleri örnekleme düşüşü nedeniyle peak yükleri göremez → riskli.
3. **Teknolojinin suistimali**
    - NILM (Non-Intrusive Load Monitoring) ile kullanıcı davranışları tahmin edilebilir → kullanıcı mahremiyeti ihlali.
4. **Yöntemlerin maliyetli olması**
    - Homomorphic encryption gerçek zamanlı çalıştırılamayabilir → ticari sistemlerde uygulama zor.