

ELEKTRİKLİ ARAÇ ŞARJ İSTASYONLARINDA OCPP TABANLI SİBER GÜVENLİK VE YAPAY ZEKA DESTEKLİ ANOMALİ TESPİTİ

Öğrenci Bilgileri

Ad Soyad: Muhammed Azizi

Öğrenci No: 190541606

Ders: Bilgi Sistemleri ve Güvenliği

Dönem: 2025 Güz

1. Proje Tanımı

Bu proje; elektrikli araç şarj istasyonlarında OCPP bağlantısının kesilmesi sırasında veya enerji akışı değerlerinde olağandışı davranışlar oluştuğunda güvenlik zafiyetlerini tespit edebilen bir simülasyon geliştirmeyi amaçlamaktadır. Sistem hem **kural tabanlı (rule-based)** hem de **makine öğrenimi tabanlı (ML-based)** hibrit anomali tespit mimarisine sahiptir.

2. Sistem Tasarımı

Geliştirilen sistem Python tabanlıdır ve kontrol arayüzü Tkinter kullanılarak oluşturulmuştur. Sistem aşağıdaki modüllerin uyumlu çalışması üzerine kuruludur:

Modül	Fonksiyon
Enerji Simülatörü	Enerji akışını üretir ve rastgele değişiklikler uygular
OCPP Durum Kontrolü	Bağlantının açık/kapalı durumunu yönetir
Replay Modülü	Kayıtlı enerji verilerini tekrar oynatır
Kural Tabanlı Kontrol	Belirlenen eşik ve kurallara göre anomali tespiti yapar
ML Tabanlı Kontrol	Normal veri üzerinden eğitilen model ile anormallikleri sınıflandırır
Log Sistemi	Tüm olayları renk kodlaması ile ekrana ve CSV dosyasına kaydeder

3. Makine Öğrenimi (ML) Bileşeni

Projede kullanılan makine öğrenimi yaklaşımı, elektriksel davranışları analiz ederek beklenmeyen enerji artışlarını tespit etmeye odaklanır.

- Model eğitim süreci **trainer.py** dosyasında gerçekleştirılmıştır
- Eğitim sonrası oluşan ML modeli **model.joblib** dosyasına kaydedilmiştir
- Çalışma zamanında model **ml_runtime.py** tarafından yüklenerek anomaly skoru hesaplanmıştır

Kullanılan algoritma: **Isolation Forest**

→ Normal davranışları "ayırmakta zorlanır", fakat anormal davranışlar hızlıca izole edilir. Bu özellik anomali tespitinde yüksek başarı sağlar.

4. Dosya ve Modül Yapısı

Dosya / Klasör	Açıklama
main.py	Simülasyonun ana akışı ve GUI
ml_runtime.py	ML modelini yükleyip anomaly kararını verir
trainer.py	Model eğitimi
model.joblib	Eğitilmiş makine öğrenimi modeli
ocpp_replay.py	Kayıtlı OCPP olaylarını yeniden oynatır
log.txt	Çalışma zamanındaki tüm olay kayıtları
normal_data.csv	Normal çalışma veri seti
rule_data.csv	Rule tabanlı anomaliler için veri seti
ocpp_log.json	Replay senaryosu dosyası

Bu modüler yapı sayesinde sistem **gerçek zamanlı, tekrarlanabilir ve analiz edilebilir** hâle getirilmiştir.

5. Kullanılan Kütüphaneler ve Gerekçeleri

Kütüphane	Görevi
Tkinter	Grafiksel kullanıcı arayüzü
threading	Çoklu iş parçacığı ve simülasyon döngüsü
pandas	CSV veri kaydı ve veri yönetimi
numpy	Sayısal hesaplamalar
scikit-learn	ML modeli (Isolation Forest)
joblib	ML modelini kaydetme ve yükleme
datetime	Zaman damgalı log üretimi
csv / json	Dosya okuma / yazma işlemleri

Ek olarak, bağımlılık yönetimi **requirements.txt** ile yapılmıştır ve proje **virtual environment** üzerinde geliştirilmiştir.
