AEGİS CHARGE

Proje Kimlik Dokümanı: AegisCharge
Proje: Bilgi Sistemleri ve Güvenliği - Elektrikli Araç Şarj Ağı Güvenliği Projesi Tarih: 4 Kasım 2025 Ekip: 6. Grup

1. Giriş

Bu doküman, "AegisCharge" projesinin temel marka kimliğini, felsefesini ve hedeflerini tanımlamak amacıyla hazırlanmıştır. Projemizin amacı, elektrikli araç şarj istasyonlarının siber güvenlik zafiyetlerini tespit etmek ve bu tehditlere karşı yapay zeka tabanlı proaktif bir savunma sistemi geliştirmektir. Bu kimlik, projemizin her aşamasında tutarlı, net ve profesyonel bir duruş sergilememiz için bize rehberlik edecektir.

2. Marka İsmi: AegisCharge

Projemizin adı "AegisCharge" olarak belirlenmiştir.

İsim Felsefesi

Bu isim, iki güçlü konseptin birleşiminden oluşmaktadır:

Aegis (Ejis): Yunan mitolojisinde "Aegis", Zeus'un koruyucu kalkanının adıdır. Bu isim, projemizin temel amacı olan "koruma", "savunma" ve "siber güvenlik kalkanı" olma rolünü doğrudan temsil etmektedir.

Charge (Şarj): Projemizin odaklandığı ana teknoloji olan "elektrikli araç şarjını" ve "enerjiyi" ifade eder.

AegisCharge, "Şarj Ederken Koruyan Kalkan" anlamını taşıyarak projemizin misyonunu tek bir kelimede özetler.

3. Logo Tasarımı

Logo Felsefesi
Logo tasarımımız, marka ismimiz olan AegisCharge'ın felsefesini görsel olarak destekler:

Kalkan Simgesi: Logonun merkezindeki kalkan, ismimizin "Aegis" bölümünü ve projemizin temel "savunma" ve "güvenlik" fonksiyonunu temsil eder.

Şimşek Simgesi: Kalkanın içindeki şimşek, "enerjiyi", "hızı" ve "şarj" (Charge) eylemini sembolize eder. Aynı zamanda, yapay zeka modelimizin siber saldırılara karşı vereceği "hızlı ve proaktif tepkiyi" de ifade eder.

Dairesel Hat: Kalkanı çevreleyen dairesel hat, tüm sistemi (ekosistemi) kapsayan, 360 derecelik tam bir koruma ağını simgeler.

Renk Paleti (Elektrik Mavisi): Seçilen teknolojik mavi tonları; "güvenilirlik", "enerji" ve "teknolojiyi" temsil eder.

4. Vizyon (Uzun Vadeli Hedefimiz)

"Tüm e-mobilite paydaşlarının (sürücüler, araçlar ve altyapı sağlayıcıları) gönül rahatlığıyla bağlandığı, %100 güvenli bir şarj ekosistemi yaratmak."

Vizyonumuzun Anlamı

Gelecekteki hedefimiz, elektrikli araç kullanımının yaygınlaşmasındaki en büyük engellerden biri olan "güvenlik" endişesini ortadan kaldırmaktır. AegisCharge, sadece bir yazılım değil, aynı zamanda tüm ekosistemin güvenle çalışmasını sağlayan bir "güven standardı" olmayı hedefler.

AegisCharge

5. Misyon (Güncel Görevimiz)

"Şarj istasyonlarının güvenlik zafiyetlerini (zayıf şifreleme, yetkisiz erişim, MitM) ortaya çıkarmak; bu zafiyetleri proaktif olarak engelleyecek yapay zeka tabanlı bir karar destek sistemi geliştirmek ve bu sistemi %95 üzerinde bir başarı oranıyla çalışır hale getirmek."

Misyonumuzun Anlamı
Misyonumuz, vizyonumuza ulaşmak için bugün attığımız net ve ölçülebilir adımları tanımlar. Görevimiz üç aşamalıdır:
Araştırmak ve Tespit Etmek: 11 kişilik ekibimizle, OCPP ve CAN Bus gibi kritik protokollerdeki 10+ özgün anomali senaryosunu araştırıp belgelemek.
Geliştirmek: Bu anomalileri tespit edebilen, öğrenebilen ve analiz edebilen akıllı bir yapay zeka (AI) modeli oluşturmak.
Başarmak: Hocamızın belirlediği başarı kriterine (minimum %95 tespit başarısı) ulaşarak, geliştirdiğimiz sistemin etkinliğini kanıtlamak.

AegisCharge

1-TEKNİK EKİP

Yapay Zeka ekibinin savunma modelini eğitebilmesi için, saldırı ve normal durumları içeren etiketli veri setlerini (CSV logları) üretip teslim ederler.

- Erkan
- Yunus
- Seher
- Eylül

2-YAPAY ZEKA EKİBİ

Model Geliştirme: Teknik ekibin ürettiği verileri kullanarak, "Normal Şarj" ile "Siber Saldırıyı" (Dalgali Yük, DoS vb.) birbirinden ayırt edebilen makine öğrenmesi algoritmasını (Random Forest) kurar ve eğitirler.

Saldırı Tespiti: Geliştirilen bu modeli kullanarak, sisteme akan canlı veriyi analiz eder ve %95 üzeri doğrulukla "Şu an saldırı var" teşhisini koyarlar.

Görselleştirme (Dashboard): Arka planda çalışan bu matematiksel sonuçları, Streamlit kütüphanesi ile hocanın ve kullanıcıların anlayabileceği, saldırı anında kırmızı alarm veren bir web arayüzüne dönüştürürler.

Muhammed Talha Kavak

Muhammed Rabiu

Sinan

Zeynep Nur

AegisCharge

3-Analiz Ekibi

Her bir saldırının sistemin hangi güvenlik açığından faydalandığını (Örn: "OCPP protokolünde şifreleme eksikliği") ve bunun yarattığı riski analiz ettiler.

Sistemin Haritasını Çizildi (UML ve Akış Diyagramları)

Sacide

Emre

Gülseren

- Teknik Ekibimiz, endüstriyel standart olan OCPP ve araç içi haberleşme protokolü CAN-bus mimarisini simüle eden bir altyapı kurdu. Bu simülasyon üzerinde,11 farklı siber saldırı senaryosunu bizzat kendimiz uyguladık.Veri oluşturduk.

Yapay zeka ekibi ile simülasyondan elde ettiğimiz bu saldırı verilerini ve normal şarj verilerini harmanladık. Yapay Zeka ekibimiz, geliştirdikleri Makine Öğrenmesi (Random Forest) modeliyle sisteme bir "beyin" kazandırdı. Bu beyin, voltajdaki milisaniyelik bir sapmayı bile analiz edip "Bu normal bir dalgalanma değil, bu bir saldırıdır!" diyebiliyor.

Analiz Ekibimiz ile tüm bu sürecin dokümantasyonunu ve risk haritalarını çıkardık.

AegisCharge

1. Adım: Sanal Motorun Çalışması (The Engine)
Sistemimiz arka planda sürekli dönen bir döngüye (Loop) sahip. Tıpkı bir arabanın motorunun rölantide çalışması gibi, bu kod saniyede bir kez tetikleniyor.
Normal Modda: Kod, matematiksel fonksiyonlar kullanarak gerçekçi elektrik verisi üretir. (Örn: Voltajı tam 220 yapmaz, 219.8 ile 220.5 arasında hafifçe titretir ki gerçekçi olsun.)
Saldırı Modunda: Senaryo devreye girer. Kod, normal veriyi bozar (Örn: Voltajı aniden 150'ye düşürür veya Akımı 0 yapar) ve bu anı Label: 1 olarak işaretler.

2. Adım: Protokol Haberleşmesi (OCPP Konuşması)

Üretilen bu veriler, sadece ekrana yazılmıyor. Sistem bu verileri OCPP 1.6 (Open Charge Point Protocol) formatında paketliyor ve WebSocket üzerinden sanal bir sunucuya (CSMS) gönderiyor.

Neden Önemli? Çünkü gerçek hayatta şarj istasyonları böyle haberleşir. Biz Excel'e elle sayı girmedik, gerçek ağ trafiğini taklit ettik.

3. Adım: Kayıt ve Çıktı (The Logger)

Trafiğin aktığı bu borunun ucunda bir "Dinleyici" (Logger) var. Bu dinleyici şunları yapıyor:

Ağdan geçen OCPP mesajını yakalıyor.

İçindeki Voltaj, Akım, Güç bilgilerini ayıklıyor (Parsing).

O an saldırı olup olmadığı bilgisini (Label) ekliyor.

Bunu saniyesi saniyesine CSV dosyasına satır satır işliyor.

YAPAY ZEKA MODELİ

AegisCharge

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
PS C:\Users\SS\Desktop\Yeni klasör\software\ml_project>

PS C:\Users\SS\Desktop\Yeni klasör\software\ml_project> python main.py
4 adet veri dosyası bulundu:
 - temiz_veri_v1.csv
 - temiz_veri_v2.csv
 - temiz_veri_v3.csv
 - temiz_veri_v4.csv

Toplam veri sayısı: 7000

DEBUG ----------------
X shape: (7000, 8)
Label dağılımı:
Label
0    3900
1    3100
Name: count, dtype: int64
----------------------

MODEL SONUÇLARI
Accuracy: 0.6257142857142857
Recall: 0.9064516129032258

Confusion Matrix:
 [[314 466]
 [ 58 562]]

Classification Report:
              precision    recall  f1-score   support

           0       0.84      0.40      0.55       780
           1       0.55      0.91      0.68       620

    accuracy                           0.63      1400
   macro avg       0.70      0.65      0.61      1400
weighted avg       0.71      0.63      0.61      1400


   macro avg       0.70      0.65      0.61      1400
weighted avg       0.71      0.63      0.61      1400
```