Hayat için Enerji

Siber Güvenlik Çalışmalarında Yapay Zekâ Metotlarının Kullanılması için Trafo Merkezi Emülatörü Geliştirmesi

Hayat için Enerji

İçerik

SCADA sistemleri, elektrik üretim tesislerinden elektrik dağıtım şebekelerine kadar birçok kritik altyapı tesisinin kontrolünü sağlar. Ancak, uzaktan erişime ihtiyaç duymaları ve kullandıkları haberleşme protokolleri nedeniyle, siber saldırılara karşı korunmaları zayıf kalabilir.

SCADA Sistemlerinin Hassasiyeti:

SCADA sistemleri, ulusal savunma örgütlerinin öncelikli endişeleri arasında yer alır. Bir petrol hattı veya elektrik santrali gibi stratejik öneme sahip tesislere yönelik siber saldırılar, ciddi can kayıplarına veya geniş çaplı kesintilere neden olabilir.

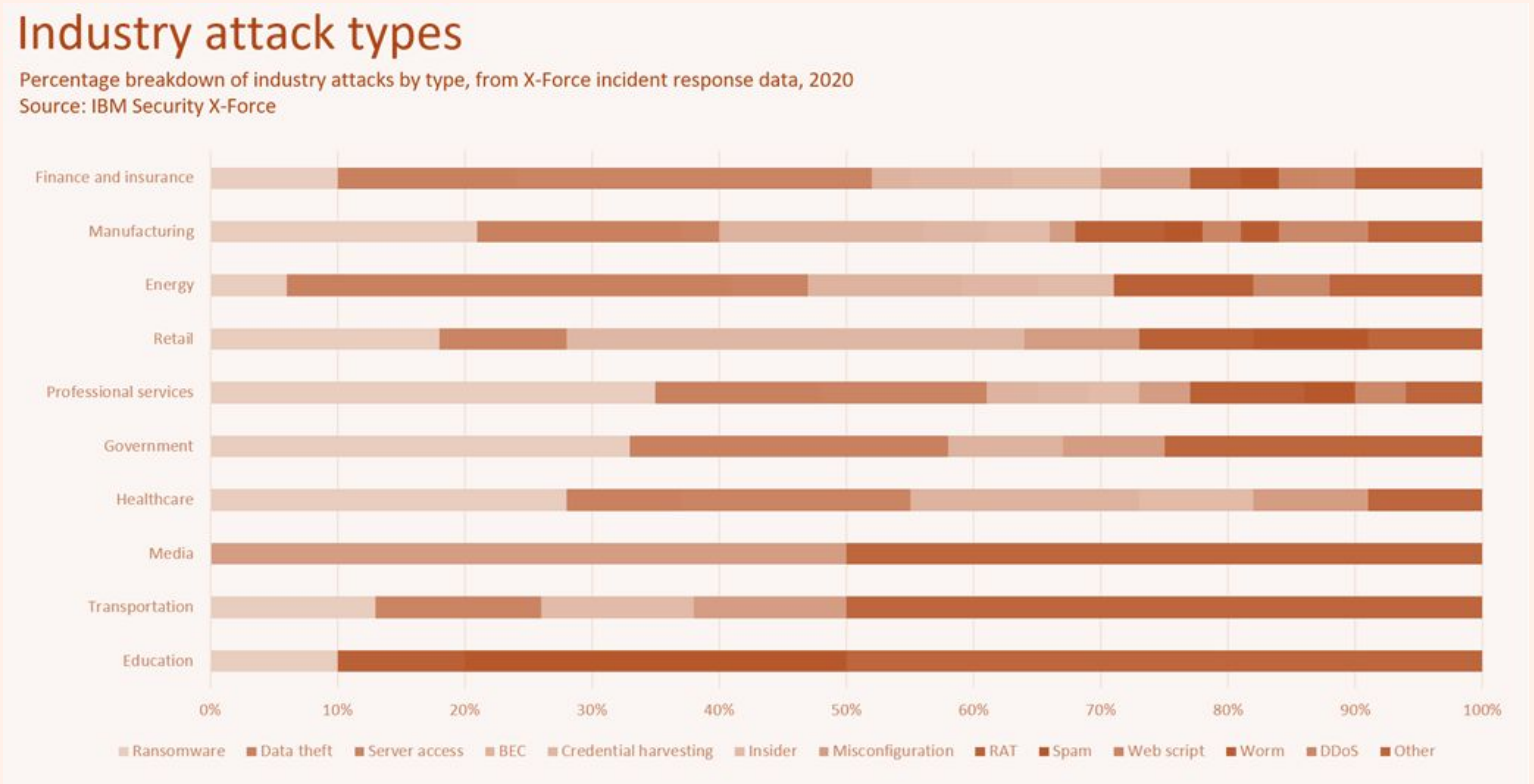
Kritik Altyapılar

Siber Saldırıların Analizi ve Saldırgan Profili:

SCADA sistemlerine yönelik siber saldırıların tespiti ve saldırgan profili hakkında yorum yapma önemlidir. Geleneksel güvenlik önlemleri, saldırı analizi veya saldırgan profili hakkında yeterli bilgi sağlamaz. Bu sistemler, siber savaşın kritik hedefleri arasında olduğundan, saldırı tipi ve saldırgan profili hakkında bilgi kritik tesisler için hayati önem taşır.

Sektörlere Göre Siber Saldırı Tipleri

Saldırganlar her sektör için farklı amaçlara sahiptir. Eğitim ve finansal kuruluşlara yapılan saldırılarda amaç kimlik bilgileri, banka bilgileri gibi verilerin toplanması iken; enerji ve üretim tesislerine yapıların saldırılarda sistemi işlemez hale getirmek en büyük amaçlar arasındadır.



Enerji Alanına Yönelik Artan Siber Tehditler

Enerji alanında faaliyet gösteren siber saldırılar son yıllarda yükselişe geçmiştir. Tabloda enerji alanına yapılan saldırılar sadece 1 yılda 6 basamak birden yükselerek en çok saldırılan 3. Sektör haline gelmiştir.

Top 10 industries ranked by attack volume, 2020 vs. 2019 | Source: IBM Security X-Force

Sector	2020 rank	2019 rank	Change
Finance and insurance	1	1	-
Manufacturing	2	8	6
Energy	3	9	6
Retail	4	2	-2
Professional services	5	5	-
Government	6	6	-
Healthcare	7	10	3
Media	8	4	-4
Transportation	9	3	-6
Education	10	7	-3

IBM Security / © 2021 IBM Corporation

ISA'nın Otomasyon ve Kontrol Sistemleri Tanımı:

Uluslararası Otomasyon Topluluğu (ISA)'na göre, otomasyon ve kontrol sistemleri, bir endüstriyel sürecin güvenli ve güvenilir çalışmasını etkileyebilecek personel, donanım ve yazılım bileşenlerini içerir.

Siber Saldırıların Endüstriyel Kontrol Sistemlerine Etkisi:

Son yıllarda, endüstriyel kontrol sistemlerini hedef alan kötü amaçlı yazılım kampanyaları artmıştır. Bu kampanyalar siber casusluk amacı taşır, çeşitli hedeflere yönelik çok yönlü ve bilgi çalma odaklıdır.

APT Yöntemleri ve Siber Casusluk:

Kullanılan kötü amaçlı yazılımlar, Gelişmiş Sürekli Tehdit (APT) yöntemlerini benimser. Yani, saldırılar, bilgi toplamak amacıyla uzun süre kurbanın sistemlerinde gizlice var olmaya çalışır ve kötü amaçlı yazılımlar keşfedilmeden önce faaliyet gösterir.

Mevcut tekniklerde farklı siber güvenlik firmalarının sunduğu geleneksel çözümler incelendiğinde; genel anlamda kural ve log tabalı bir çözüm sundukları ancak SCADA ağını saldırılara karşı korumak için yeterli çözümü sağlamadıkları gözlemlenmiştir.

Yeni tekniklerde, iç ağdaki ajan yazılımlar aracılığıyla sistemin performansını ve güvenliğini denetlemeyi amaçlayan bir yaklaşım öne çıkmaktadır. Belirli değerlere göre sistem alarm verme prensibine dayalı bir yapı söz konusudur.

SCADA networkünde kullanılan teknikler, ilk gözlenen değerlere dayalı olarak anomalileri tespit eden bir yöntemi benimser. Ayrıca, endüstriyel kontrol sistemleri için siber güvenlik yönetimini geliştirmek amacıyla, bir SCADA'ya entegre edilmiş bir merkezi Sistem Güvenlik Yöneticisi bulunmaktadır. Bu yöntem, endüstriyel kontrol sistemlerinin güvenlik durumuyla ilgili verileri toplamak ve yönetmek için kullanılır.

SCADA networkünde cihazların whitelist'lerini oluşturarak, bu bilgileri bir veritabanında saklayan ve sürekli olarak SCADA konfigürasyonuna göre saldırı tespit ve engelleme sistemini güncelleyen bir yöntem kullanılmıştır.

Çalışma, yapay zeka modellerinin anomal trafiği tespit edebilmesi için bir trafo merkezi simülasyon ortamından normal çalışma alanındaki network paketlerinin toplanması ve anormal veri paketlerinin oluşturulmasını hedeflemiştir.

Sanallaştırma ve Protokoller:

Mevcut hiyerarşik SCADA sistemleri, dahili güvenlik mekanizmasına sahip olmayan iletişim protokollerini kullanır. Çalışmada IEC 60870-5-101 ve IEC 60870-5-104 protokollerinin zayıf noktaları tespit edilmiştir.

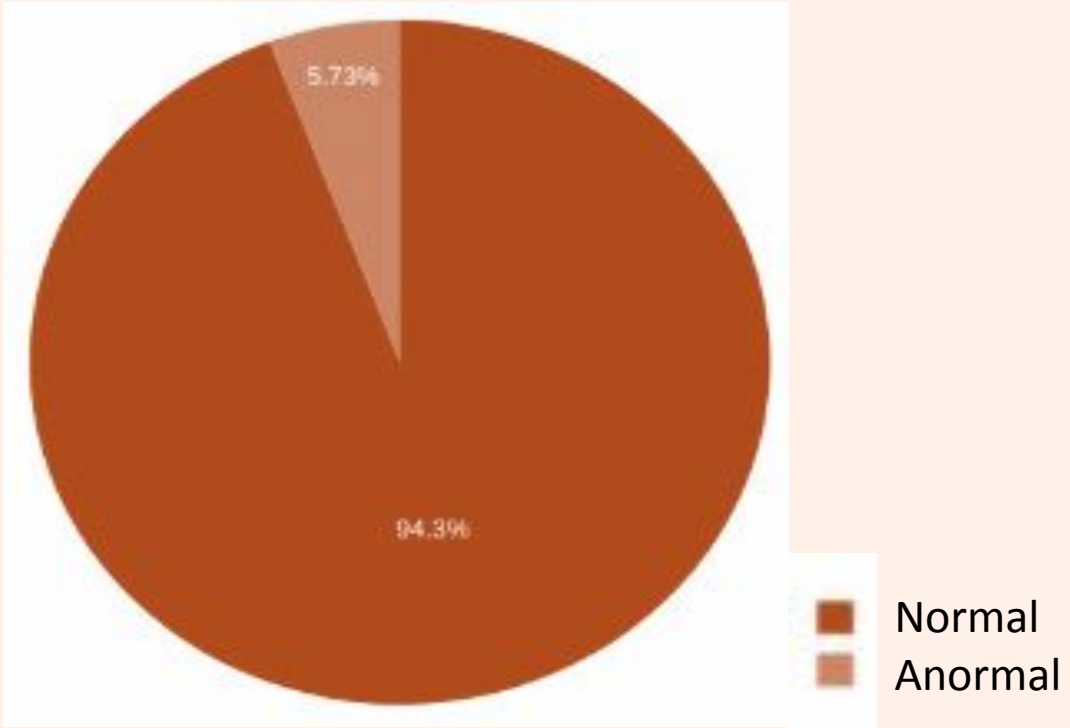
Veri Toplama ve Analiz Süreci:

IEC 60870-5-104 protokolü ile trafo merkezleri ve üretim santrallerinden veri toplanmış ve bu veriler farklı cihazlar tarafından farklı protokollerle okunarak IEC 60870-5-104 protokolüne dönüştürülmüştür.

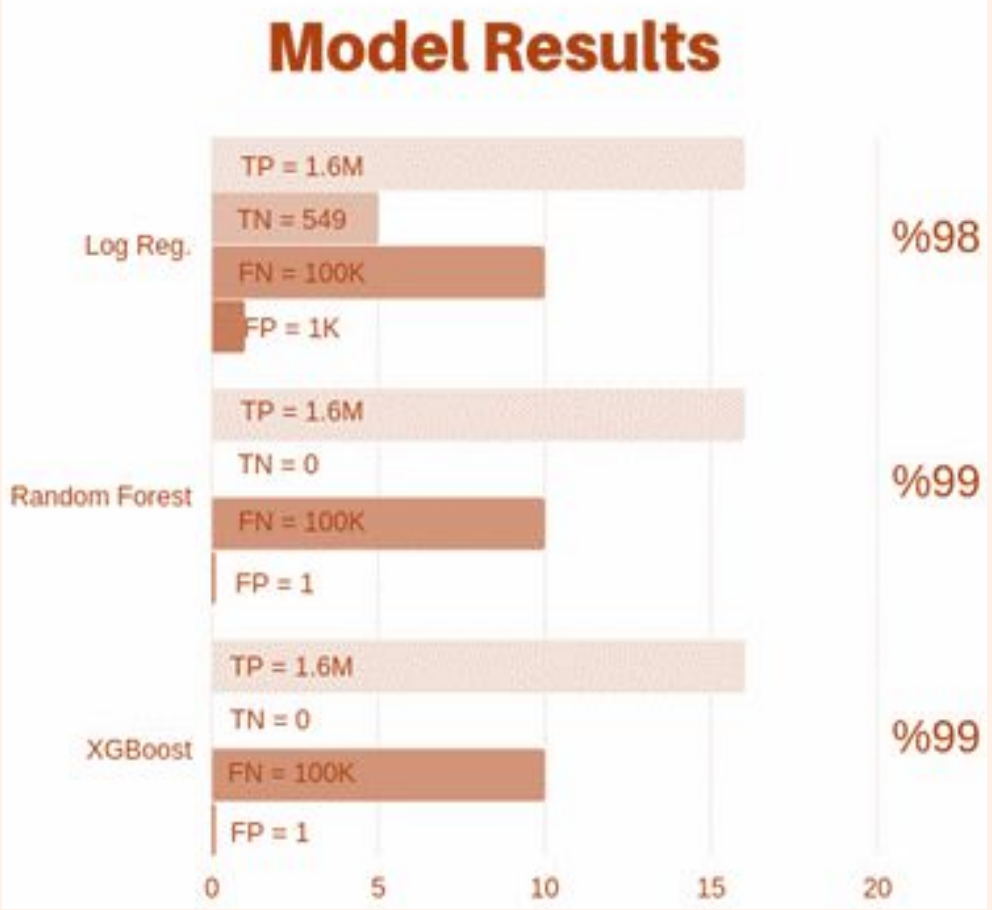
Özellik Çıkarımı ve Veri Temizleme:

Çalışmada örnek veri seti üzerinde temiz veri oluşturulmuştur. 25 özellikten oluşan veri, 7 özelliğe indirgenerek temizlenmiştir. Bu temizleme sürecinde kayıp, bozuk ve aykırı veriler temizlenmiştir.

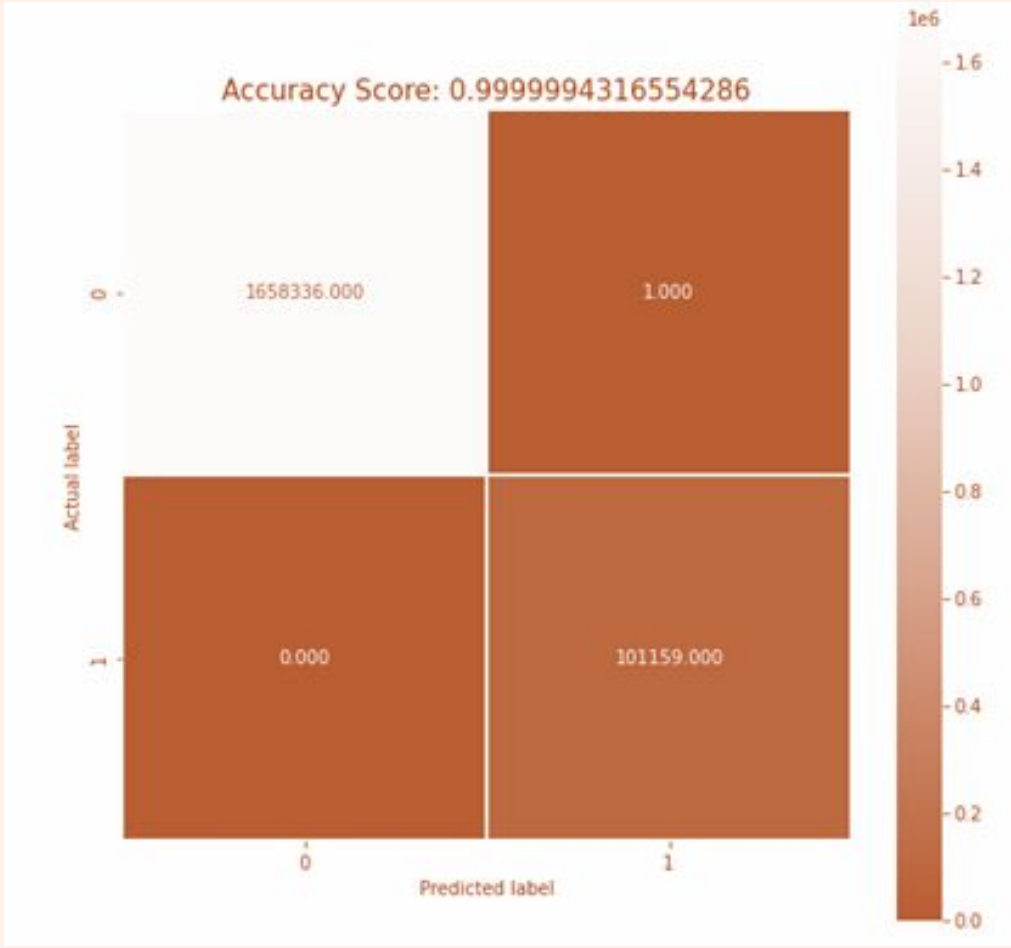
Target yani verilerin normal ve anormal olduğunu temsil eden etiket verisi içerisinde veri normal ve anormal olarak iki ayrı sınıf taşımaktadır. Normal ve anormal verilerin dağılımları aşağıdaki şekilde gösterilmektedir.



Özniteliklerin belirlenmesi çalışması yapılırken ilk önce NSL-KDD public veri seti kullanılmıştır. Çalışma kapsamında toplamda 22540 farklı train datası kullanılarak model eğitilmiştir. NSL-KDD veri setinde "normal" ve "anormal" olarak etiketlenen verilerden anomali tespiti yapılması için gereken model oluşturulmuştur. Anormal veri setine dahil edilen veriler 4 farklı kategoride etiketlenerek alt kategoriler oluşturulmuştur. Modeller üzerinde K-fold cross validation yapılarak, NSL-KDD veri seti üzerinde Logistic Regression, Support Vector Machine(SVM), KNN algoritmalarının anomali tespitindeki başarı değerleri hesaplanmış yandaki sonuçlar elde edilmiştir. Yapay zeka çalışmalarında Python dili tercih edilmiştir. Bu kapsamda çalışılan makine öğrenmesi modelleri: KNN, Logistic Regression, Mean Shift, One Class SVM, Random Forest, SVM.



Performans ve doğruluk oranı olarak en başarılı XGBoost modelinin confusion matrix sonuçlarına aşağıdaki şekilde yer verilmiştir.

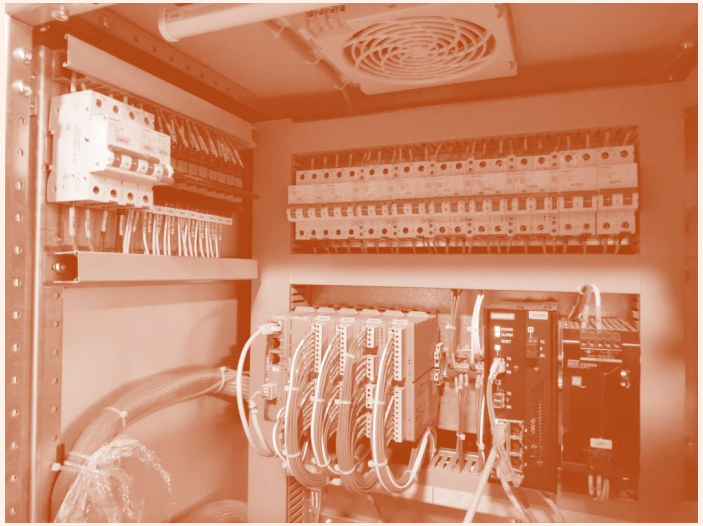


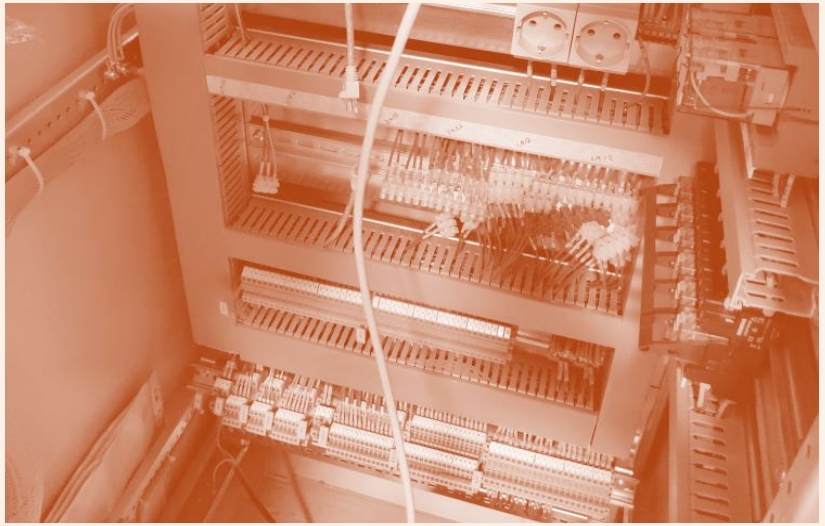
Araştırma Hedefi:

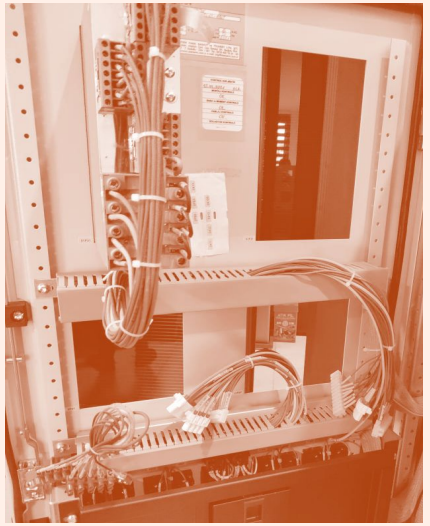
Çalışma, kritik altyapı tesislerinde kullanılan SCADA sistemlerinin güvenliğini artırmak amacıyla yapılmıştır. Özellikle IEC-104 protokolünde tespit edilen zafiyetler üzerinde odaklanılmıştır.

Sistemde Yapılan İyileştirmeler:

İnceleme sonucunda belirlenen zafiyetlere yönelik bir kontrol mekanizması geliştirilmiştir. Bu mekanizma, IEC-104 protokolüne dışarıdan yetkisiz müdahaleleri engellerken, sistem içinde değerlerin kontrol altına alınmasını sağlamıştır.







Yapay Zeka ile Güvenlik Analizi:

Yapay zeka ile eğitilen sistem, farklı atakları içeren bir veri kümesi üzerinde çalışmış ve bu atakları tespit etme başarısını Logistic Regression, Support Vector Machine(SVM), KNN, XGBoost gibi algoritmalarla değerlendirmiştir. En yüksek sınıflandırma oranına XGBoost Algoritması sahip olmuştur.

Gelecek İçin Öneriler ve Çalışma Alanı:

Elektrik kontrol sistemlerinin haberleşme protokollerinin güvenlik açısından yeniden değerlendirilmesi ve siber güvenlik açısından ele alınması gerekliliği vurgulanmıştır. Gelecekte, farklı veri kümeleri ile daha kapsamlı siber terör ataklarının analizi yapılmalı ve bu alandaki araştırmalar genişletilmelidir.

Önemli Sonuç:

Elektrik üretim, iletim ve dağıtımına ilişkin kontrol sistemlerinin güvenliği, özellikle SCADA sistemleri için hayati derecede önemlidir. Sunulan çalışmanın, SCADA sistemlerinin güvenliği üzerine yapılacak çalışmalara katkı sağlayabileceği değerlendirilmektedir.

Bu çalışma EPDK tarafından 15.03.2019 tarihli 01/19/03-2 numaralı komisyon kararı ile desteklenen ve ADM EDAŞ ve GDZ EDAŞ firmalarının birlikte gerçekleştirdikleri “Siber Güvenlik Çalışmalarında Yapay Zeka Metodlarının Kullanılması için Trafo Merkezi Emülatörü Geliştirme” Ar-Ge projesi kapsamında desteklenmiştir.

Hayat için enerji

Teşekkürler

Sude Kozalıoğlu
Ar-Ge Mühendisi

Denizli - Türkiye
T 0258 296 7000 – 538 449 29 99
E sude.kozalioglu@admelektrik.com.tr
www.admelektrik.com.tr

Energy for Life

[1] https://www.dell.com/downloads/global/solutions/2014_DSAT_Report_Final.pdf
[2] GICSP, E. H. , Assante , M., & Conway , T. (2014). An abbreviated history of automation & industrial controls systems and cybersecurity . SANS Institute , Tech . Rep .
[3] Wangen , G. (2015). The role of malware in reported cyber espionage : a review of the impact and mechanism _ Information, 6(2), 183-211.
[4] Skare PM (2009) . method and system for cyber security management of industry control systems US Patent No. 2007/294369
[5] Naedele M. , Biderbost O. (2004). network security system E. Patent No. 1544707
[6] Falavigna L. , Bima C. (2007) Industrial plant security apparatus and monitoring method of security of an industrial plant E. Patent No. 1881388
[7] AROV M., OCHMAN R., Cohen M. (2016) System and method for detecting a cyber-attack at scada / ics managed plants WO Patent No. 2017/090045