Güç Sistemlerine Yönelik Derin Öğrenme Tabanlı Saldırı Tespit Sistemi

Deep Learning Based Intrusion Detection System for Power Systems

Hamdullah KARAMOLLAOĞLU[1], İbrahim YÜCEDAĞ[2], İbrahim Alper DOĞRU[3]

[1]Elektrik Üretim A.Ş., EYS ve Eğitim Daire Başkanlığı
h.karamollaoglu@euas.gov.tr

[2]Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği
ibrahimyucedag@duzce.edu.tr

[3]Gazi Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği
iadogru@gazi.edu.tr

Özet

Bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte bu teknolojilerin kritik altyapıları izleyen ve kontrol eden Endüstriyel Kontrol Sistemleri'ne (EKS) entegrasyonu da hız kazanmıştır. EKS'ler ile iletişim teknolojilerinin birlikte kullanılması, EKS'lere yönelik siber saldırılarda artışa neden olmuştur. Bu nedenle EKS sistemlerinin işleyişini etkileyebilecek, maddi ve manevi kayıplara neden olabilecek saldırıları tespit edebilen sistemlerin geliştirilmesi her geçen gün daha fazla önem kazanmaktadır. Bu çalışmada, Temel Bileşenler Analizi (PCA), Sentetik Azınlık Aşırı Örnekleme Yöntemi (SMOTE) ve Evrişimsel Sinir Ağları *(CNN) yöntemlerinin birlikte kullanıldığı bir model yardımıyla güç sistemlerinde kullanılan EKS'ler için bir saldırı tespit sistemi (STS) önerilmiştir. Geliştirilen STS'nin performans testi çeşitli veri setleri üzerinde gerçekleştirilmiştir. Sınıflandırma sonucunda %92,75'e varan tespit doğruluğu elde edilmiştir.*

Anahtar kelimeler: *EKS, güç sistemleri, saldırı tespit sistemi, SCADA, STS*

Abstract

With the development of information and communication technologies, the integration of these technologies into ICS systems that monitor and control critical infrastructures has also gained momentum. The combined use of ICSs and communication technologies causes an increase in cyber attacks against ICSs. For this reason, the development of systems that can detect attacks that may affect the operation of ICS systems and cause material and moral losses is gaining more importance with each passing day. In this study, an intrusion detection system (IDS) is proposed for ICSs used in power systems with the help of a model in which Principal Components Analysis (PCA), Synthetic Minority Oversampling Technique (SMOTE) and Convolutional Neural Network (CNN) methods are used together. The performance test of the developed IDS was carried out on various datasets. As a result of classification, detection accuracy up to 92,75% was obtained.

Keywords: *ICS, power systems, intrusion detection system, SCADA, IDS,*

1. Giriş

Günümüzde bilgi ve iletişim teknolojilerinin hızla gelişmesi ile birlikte Endüstriyel Kontrol Sistemleri de bu teknolojiler ile entegre olmuş ve yeni nesil ağ tabanlı EKS'lerin kritik altyapıların izlenmesi ve kontrolünde kullanımı hız kazanmıştır. Elektrik üretim santrallerinden, sağlık sistemine; su şebekelerinden raylı ulaşım sistemlerine kadar her türlü kritik altyapıda kullanılan yeni nesil EKS'ler de internete erişimi olan her sistem gibi siber saldırılara maruz kalmaktadır. Siber saldırılar sonucunda zarar gören ve işlevini yerine getiremeyen EKS'ler çok ciddi maddi ve manevi kayıplara sebep olabilmektedir [1,2].

EKS'lere yönelik saldırılar genellikle veri enjeksiyonu, zayıf kimlik doğrulama, sosyal mühendislik, bellek taşırma, kötü amaçlı yazılımlar yolu ile yapılan saldırılar, sıfır gün saldırıları, DoS/DDoS saldırıları, haberleşme kanalı ve haberleşme protokolleri açıklıkları üzerinden gerçekleştirilen saldırılardır [3,4]. İmza tabanlı (klasik antivirüsler vs.) sistemler ile bu saldırıların tespitinde güçlükler yaşanmaktadır. Günümüzde imza tabanlı saldırı sistemlerinin yanı sıra, anomali tabanlı sistemler de EKS'lere yönelik saldırıların tespitinde kullanılmaktadır. Anomali tabanlı saldırı tespit sistemlerinde, makine öğrenmesi ve derin öğrenme vb.

yöntemler yardımıyla EKS'lerin davranışları analiz edilerek saldırı tespit sistemi eğitilmekte, EKS ağı üzerinde meydana gelen anormal bir davranışta uyarı sinyali oluşturularak sistem yöneticisi bilgilendirilmektedir. Bu çalışmada derin öğrenme yöntemlerinden Evrişimli Sinir Ağları (CNN) kullanılarak anomali tabanlı bir saldırı tespit sistemi geliştirilmiştir. Tasarlanan sistemin saldırıları doğru bir şekilde tespit edebilmesinin yanı sıra, mümkün olan en hızlı şekilde ve en az maliyetle sınıflandırma işleminin gerçekleştirilmesi önem arz etmektedir. Çalışmada saldırı tespit sistemi için önerilen modelde Evrişimli Sinir Ağları'nın yanı sıra, veri indirgeme için Temel Bileşenler Analizi metodu, verisetlerindeki dengesiz sınıf dağılımlarının önüne geçebilmek için ise SMOTE yöntemi kullanılmıştır.

Çalışmanın ikinci bölümünde literatür taraması gerçekleştirilmiş, üçüncü bölümde materyal ve metot sunulmuş, dördüncü bölümde deneysel çalışma üzerinde durulmuş, son bölümde ise elde edilen sonuçlar ve genel değerlendirme yapılmıştır.

2. İlgili Çalışmalar

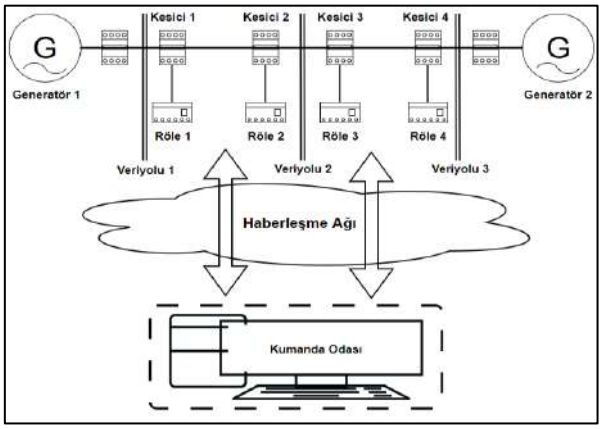
Kritik altyapıların güvenliğinin sağlanmasına önemli role sahip olan saldırı tespit sistemlerinin geliştirilmesine yönelik çalışmalar yeni nesil akıllı EKS sistemlerinin ortaya çıkması ile beraber ivme kazanmıştır. Yapılan çalışmalar incelendiğinde imza tabanlı saldırı sistemlerinin yanı sıra son yıllarda özellikle anomali tabanlı saldırı tespit sistemlerinin bu alandaki en önemli araştırma konuları arasında yer aldığı görülmektedir.

Benisha ve Ratna [5] tarafından rüzgâr türbinlerinin izlenmesi ve kontrolünde kullanılan SCADA sistemlerine yönelik olarak geliştirilen saldırı tespit sisteminde EELM ve MGWO yöntemleri kullanılmıştır. Sistemin performans testi için gerçek zamanlı rüzgâr türbini verilerinden oluşturulmuş ve 76 öznitelik içeren bir veriseti kullanılmıştır. Sonuçta, %97,6 oranında doğruluk ile saldırı sınıflandırması gerçekleştirilmiştir. Khan vd. [6] tarafından doğalgaz boru hattı sistemlerine yönelik olarak geliştirilen saldırı tespit sisteminde sınıflandırma için kNN, öznitelik indirgeme için PCA, CCA ve ICA, verisetini dengeli hale getirmek için ise SMOTE yönteminin kullanıldığı hibrit bir model önerilmiştir. Çalışmanın eğitim ve test işlemleri Mississippi Üniversitesi tarafından oluşturulmuş gaz boru hattı sistemi veriseti [7] kullanılarak gerçekleştirilmiştir. Sonuçta %97'lik doğruluk oranı ile sınıflandırma gerçekleştirilmiştir. Gao vd. [8] tarafından derin öğrenme yöntemlerinden LSTM ve FNN'nin birlikte kullanıldığı bir topluluk öğrenme yöntemi ile SCADA sistemlerine yönelik saldırı tespit sistemi geliştirilmiştir. Stewart vd. [9] EKS sistemlerine yönelik olarak geliştirdikleri saldırı tespit sisteminde OCSVM yöntemini kullanmışlardır. Teixeira vd. [10] su tankının su seviyesini izleyen ve kontrol eden bir SCADA sistemine yönelik olarak ANN metodu yardımıyla bir saldırı tespit sistemi geliştirmişlerdir. Chu vd. [11] tarafından haberleşme için Modbus protokolünü kullanan SCADA sistemleri için geliştirilen saldırı tespit sisteminde GoogleNet-LSTM tabanlı hibrit bir model kullanılmıştır. Kasongo vd. [12] tarafından SCADA sistemlerine yönelik olarak önerilen saldırı tespit sisteminde öznitelik seçimi için IG metodu, sınıflandırma için ise GRU derin öğrenme yöntemi kullanılmıştır.

Literatürdeki çalışmalar incelendiğinde EKS sistemlerine yönelik olarak geliştirilen saldırı tespit sistemlerinde genellikle hibrit yapıdaki makine öğrenmesi yöntemleri ve derin öğrenme yöntemlerinin kullanıldığı görülmektedir.

3. Materyal ve Metot

Çalışmada 15 farklı 'csv' uzantılı dosyadan oluşan güç sistemlerine yönelik saldırı verisetleri (DATA-1, DATA-2,…,DATA-15) kullanılmıştır. Bu verisetleri Mississippi Üniversitesi ve Oak Ridge Ulusal Laboratuvarı tarafından, temel yapısı Şekil 1'de sunulan gerçek zamanlı bir güç sistemi simülatörünün davranışları izlenerek oluşturulmuştur [13].



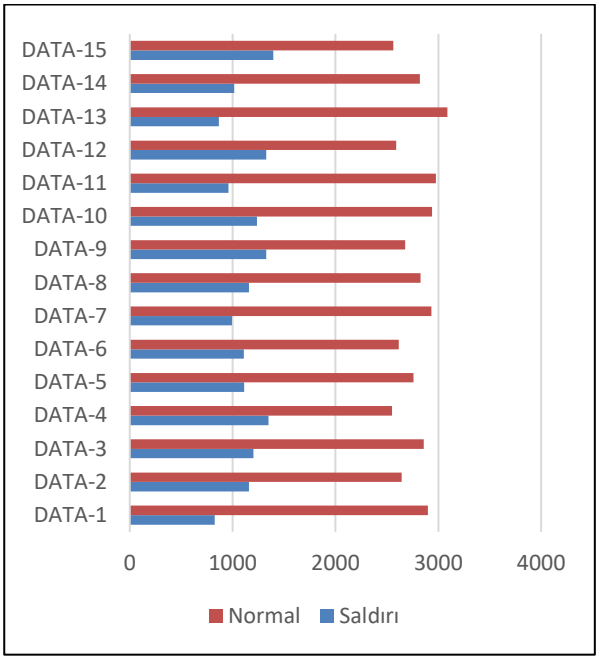
Şekil 1. Güç sistemi temel yapısı

Şekil 1'deki güç sistemde yer alan 4 adet akıllı röle içerisine dahil edilmiş 4 adet fazör ölçüm biriminin (FÖB) her biri ile 29 farklı ölçüm yapılarak toplam 116 adet öznitelik çıkarımı gerçekleştirilmiştir. Röleler ile haberleşmede Modbus protokolü kullanılırken, FÖB'ler için IEEE C37.118 protokolü kullanılmaktadır [14]. Verisetlerinde FÖB'lerden elde edilen öznitelik tipleri Tablo 1'de görüldüğü gibidir.

Tablo 1. FÖB'lerden elde edilen öznitelik tipleri

Öznitelik	Açıklama
PA1-PA3	Faz A-C Gerilim faz Açısı
PM1-PM3	Faz A-C Voltaj faz büyüklüğü
PA4-PA6	Faz A-C Mevcut faz açısı
PM4-PM6	Faz A-C Mevcut faz büyüklüğü
PA7-PA9	Poz-Neg.-Sıfır gerilim faz Açısı
PM7-PM9	Poz-Neg.-Sıfır gerilim faz büyüklüğü
PA10-PA12	Poz-Neg.-Sıfır akım faz açısı
PM10-PM12	Poz-Neg.-Sıfır akım faz büyüklüğü
F	Röleler için frekans değeri
DF	Röleler için frekans değişim oranı (df/dt)
PA-z	Röleler için empedansı değeri
PA-zh	Röleler için empedans açısı
S	Röleler için durum bayrağı

Tablo 1'de yer alan öznitelikler haricinde verisetinde yer alan diğer 12 öznitelik ise kontrol paneli ve 4 adet röleden elde edilen kayıtlar ile Snort uyarı sinyallerine ait değerleri içermektedir. Verisetlerinde yer alan her bir örnek 'Normal' ve 'Saldırı' olmak üzere iki sınıfta etiketlenmiştir. Verisetlerinde yer alan örnek sayılarının dağılımı Şekil 2'de görüldüğü gibidir.



Şekil 2. Verisetlerindeki veri dağılımları

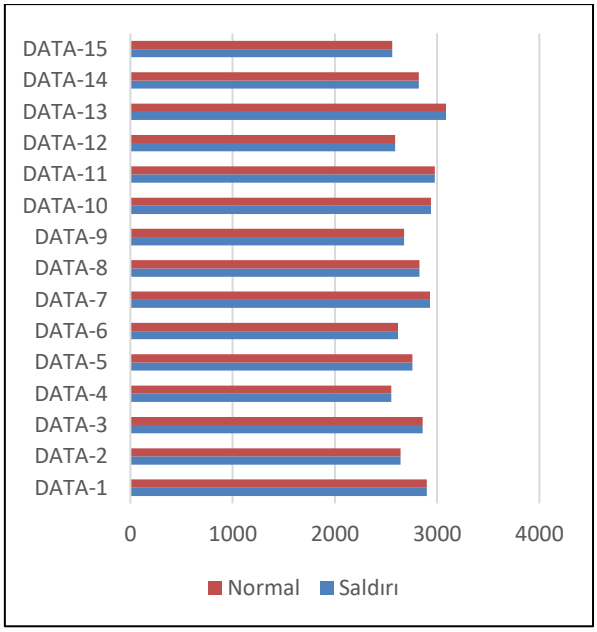
Şekil 2 incelendiğinde her bir verisetinde 'Normal' olarak etiketlenmiş verilerin sayısının 'Saldırı' olarak etiketlenmiş örneklerin sayısından bir hayli fazla olduğu görülmektedir. Bu durum verisetlerinde sınıf dengesizliği problemine sebep olmakta ve saldırı tespitinde kullanılan Makine Öğrenmesi ve Derin Öğrenme yöntemlerinin azınlık sınıflarda yer alan örneklerin hatalı sınıflandırılmasına yol açmaktadır. Bu çalışmada, dengesiz sınıf dağılımının giderilmesi için Sentetik Azınlık Aşırı Örnekleme (SMOTE) yönteminden yararlanılmıştır.

3.1. Sentetik Azınlık Aşırı Örnekleme Yöntemi (Synthetic minority oversampling technique-SMOTE)

Verisetlerindeki sınıflarda yer alan verilerin dağılımını dengeli hale getirmek için kullanılan bu yöntemde, yeni sentetik veriler üretilerek, bu örneklerin azınlık sınıfa dahil edilmesi işlemi gerçekleştirilmektedir. Sentetik örnek üretme işlemi azınlık sınıftaki örnek sayısı çoğunluk sınıftaki örnek sayısına eşit oluncaya kadar devam eder. Bu yöntemde ilk olarak örnek uzayda Öklit yöntemi yardımıyla azınlık sınıfında yer alan her bir örneğin (x_i) k adet en yakın komşusu (kNN) belirlenmektedir. Sonrasında belirlenen k adet komşu örnek içerisinden rastgele olarak bir örnek (x_j) seçilmekte ve yeni sentetik örnek (x_s), x_i ile x_j arasında konumlandırılmak üzere Denklem 1 yardımı ile elde edilmektedir [15, 16].

$$x_s = (x_i - x_j) \cdot r \; ; \; r \in [0,1] \qquad (1)$$

Denklem 1'deki r değeri 0-1 arasında üretilen rastgele bir sayıdır. Çalışmada ele alınan 15 adet veriseti üzerinde SMOTE yönteminin uygulanması sonucunda elde edilen yeni dengeli verisetlerine ait veri dağılımları Şekil 3'te görüldüğü gibidir.

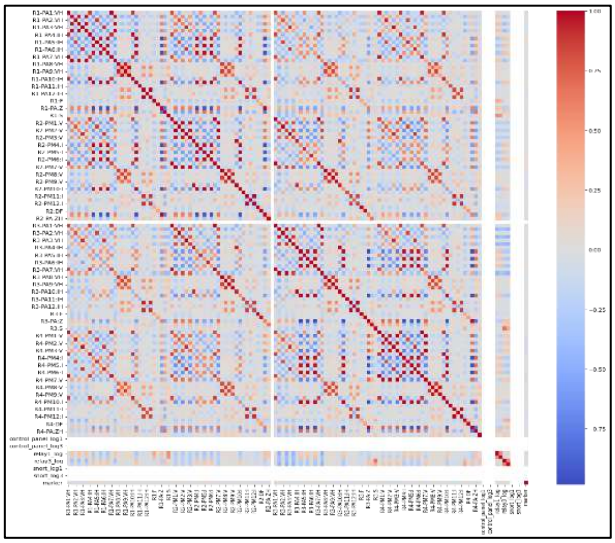


Şekil 3. SMOTE sonrası elde edilen veri dağılımları

Şekil 3'te görüldüğü gibi SMOTE yöntemi sonucunda sınıflar arasındaki veri dengesizliği sorunu giderilmiş ve verisellerinde yer alan azınlık sınıf (Saldırı) ile çoğunluk sınıf (Normal) arasındaki örnek sayıları eşitlenmiştir.

3.2. Temel Bileşenler Analizi (Principal Component Analysis-PCA)

Verisetinde yer alan 128 adet öznitelik arasındaki kolerasyon Şekil 4'te yer alan ısı haritası yardımıyla görülebilmektedir.



Şekil 4. Öznitelikler için Isı Haritası

Şekil 4'te görüldüğü gibi bazı öznitelikler arasındaki kolerasyon değeri çok yüksek seviyededir. Çalışmada Temel Bileşenler Analizi (PCA) yöntemi [17] kullanılarak kolerasyonu yüksek olan öznitelikler bir araya getirilmek suretiyle temel bileşenler olarak nitelendirilen ve doğrusal olarak ilişkisiz olan daha az sayıda yapay değişkene dönüştürülmektedir. Bu sayede varyansı en yüksek oranda tutup, daha az öznitelik ve en az bilgi kaybı ile verisetindeki verilerin temsil edilmesi sağlanmıştır.

PCA yöntemi ile gerçekleştirilen öznitelik indirgenmesi sayesinde saldırı sınıflandırması için derin öğrenme ve makine öğrenmesi yöntemlerinin kullanımı sırasında CPU kullanım maliyeti ve sınıflandırma süresi azaltılmaktadır. Çalışmada ele alınan her bir verisetindeki verilerin temsilinde varyans oranını %99 oranında sağlayacak kadar temel bileşen kullanılmıştır. Sonuçta her bir veriseti için elde edilen temel bileşen sayıları Tablo 2'de görülmektedir.

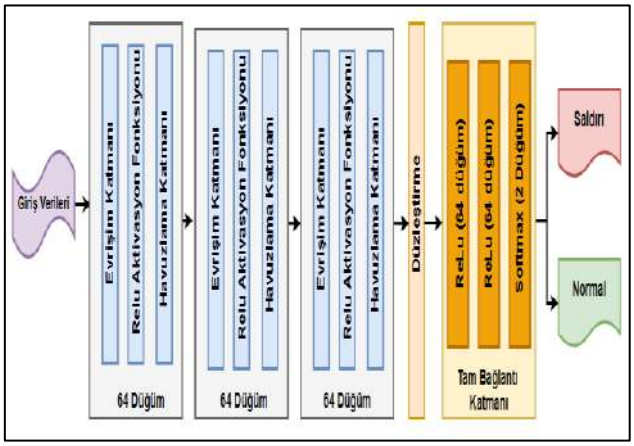
Tablo 2. PCA ile elde edilen temel bileşen sayıları

Veriseti	Temel Bileşen Sayısı
DATA-1	51
DATA-2	51
DATA-3	51
DATA-4	51
DATA-5	52
DATA-6	52
DATA-7	51
DATA-8	52
DATA-9	52
DATA-10	53
DATA-11	52
DATA-12	50
DATA-13	54
DATA-14	52
DATA-15	51

Tablo 2'de görüldüğü gibi PCA yöntemi sayesinde verisetlerinde yer alan 128 olan öznitelik, 51 ile 54 arasında değişen sayıda temel bileşen ve %99 varyans oranı ile temsil edilmiştir. Böylelikle eğitim ve test işlemleri için derin öğrenme yöntemlerinde kullanılacak öznitelik sayısı yarıdan daha aza indirgenerek en az bilgi kaybı ile modelin eğitim ve saldırıları tespit etme süresi azaltılmıştır.

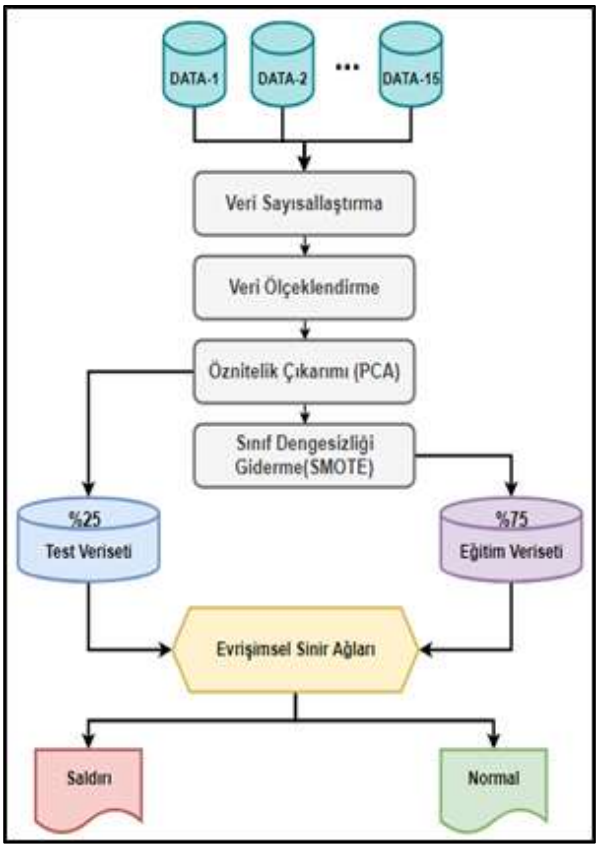
3.3. Evrişimsel Sinir Ağları (Convolutional Neural Networks-CNN)

Çalışmada ele alınan verisetlerindeki örneklerin %75'i eğitim, kalan %25'i ise geliştirilen saldırı tespit sisteminin performans testi için ayrılmıştır. Verisetlerinde yer alan örneklerin sınıflandırılması aşamasında Derin Öğrenme yöntemlerinden Evrişimsel Sinir Ağları (CNN) yöntemi [18] kullanılmıştır. Kullanılan CNN yönteminin mimari yapısı Şekil 5'te görülmektedir.



Şekil 5. Kullanılan CNN yönteminin mimari yapısı

Şekil 5'te görüldüğü gibi tasarlanan CNN'nin yapısında 3 adet 64 düğümlü Evrişimsel katman ile 3 adet Tam Bağlantı katmanı yer almaktadır. Evrişimsel katmanda aktivasyon fonksiyonu olarak ReLU, boyut indirgeme/filtereleme işlemi için ise Maksimum Havuzlama katmanı kullanılmıştır. Evrişimsel katmanlardan geçen örnekler Düzleştirme katmanı ile tek düzlemli hale dönüştürüldükten sonra Tam Bağlantı katmanına girmektedir. Tam Bağlantı katmanında 64 düğümden oluşan ve ReLU aktivasyon fonksiyonu içeren 2 adet Dense katmanı ile 2 düğümden oluşan ve Softmax fonksiyonu içeren 1 adet Dense katmanı yer almaktadır. Tam bağlantı katmanının ardından örnekler Saldırı veya Normal olarak sınıflandırılmaktadır. Saldırı Tespit Sistemi'nin akış diyagramı Şekil 6'da görülmektedir.



Şekil 6. Saldırı Tespit Sistemi'nin mimari yapısı

Şekil 6'da görüldüğü gibi ön-işlem, öznitelik çıkarımı, sınıf dengesizliğinin giderilmesi işlemlerinin ardından verisetlerinde yer alan örnekler CNN yardımıyla sınıflandırmaya tabii tutulmuştur.

4. Deneysel Çalışma

Çalışmada ele alınan 15 adet güç sistemlerine yönelik olarak oluşturulmuş saldırı verisetleri üzerinde PCA, SMOTE ve CNN yöntemleri kullanılarak geliştirilen saldırı tespit sisteminin performans değerlendirmesinde Doğruluk, Kesinlik, Duyarlılık ve F1-Skoru performans ölçütleri kullanılmıştır. Elde edilen sonuç performans ölçüm değerleri Tablo 3'te görüldüğü gibidir.

Tablo 3. Sonuç performans değerleri

Veriseti	Doğruluk	Kesinlik	Duyarlılık	F1-skoru
DATA-1	0,9275	0,8914	0,9014	0,89625
DATA-2	0,8762	0,8537	0,85415	0,8539
DATA-3	0,8936	0,8714	0,8746	0,873
DATA-4	0,8716	0,8607	0,85315	0,8567
DATA-5	0,8978	0,8796	0,8669	0,8729
DATA-6	0,8841	0,8683	0,8487	0,8575
DATA-7	0,9137	0,88205	0,8933	0,88745
DATA-8	0,8751	0,8466	0,85385	0,85005
DATA-9	0,8801	0,8685	0,8579	0,8628
DATA-10	0,8808	0,85825	0,85415	0,85615
DATA-11	0,8873	0,85835	0,8264	0,84055
DATA-12	0,8737	0,8697	0,8434	0,85425
DATA-13	0,9006	0,85275	0,85885	0,85575
DATA-14	0,8663	0,82555	0,83805	0,8314
DATA-15	0,8749	0,86405	0,8608	0,86235

Tablo 3'teki performans değerleri incelendiğinde verisetleri üzerinde gerçekleştirilen sınıflandırma sonucunda en yüksek doğruluk oranının DATA-1 veriseti ile %92,75 olarak elde edildiği görülmektedir.

5. Sonuçlar ve Değerlendirme

Bilgi ve haberleşme teknolojilerinin kritik altyapılarda kullanımındaki hızlı artış, bu altyapıların izleme ve kontrolü için kullanılan yeni nesil ağ tabanlı EKS sistemlerine yönelik saldırılarda da artışa neden olmuştur. Bu çalışmada güç sistemlerine yönelik olarak EKS'ler için bir saldırı tespit sistemi sunulmuştur. Önerilen STS modeli PCA, SMOTE ve CNN yöntemleri birlikte kullanılarak geliştirilmiştir.

Saldırı tespit sistemlerinde, saldırı tespit hızı da tespit doğruluğu kadar önem arz etmektedir. Çalışmada bu amaçla PCA yöntemi kullanılarak en az öznitelik ve en yüksek varyans ile verisetleri temsil edilmeye çalışılmıştır. Ayrıca SMOTE yöntemi ile verisetlerinde yer alan sınıflardaki dengesiz veri dağılımları dengeli hale getirilmiştir. Çalışmada ele alınan verisetleri kullanılarak gerçekleştirilen performans testi sonucunda %92,75'e varan doğruluk oranları elde edilmiştir.

Gelecekte saldırı sınıflandırmasında kullanılan derin öğrenme yöntemlerin bir arada kullanıldığı hibrit yapıdaki modeller yardımıyla kritik altyapılarda kullanılan EKS sistemlerine yönelik saldırı tespit sistemlerinin geliştirilmesi amaçlanmaktadır.

6. Kaynaklar

[1] Söğüt, E., Erdem, O. A. "Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi." *Politeknik Dergisi*, 23(2), 557-566, 2020.

[2] Irmak, E., Erkek, İ. "Endüstriyel Kontrol Sistemleri ve SCADA Uygulamalarının Siber Güvenliği: Modbus TCP Protokolü Örneği." *Gazi University Journal of Science Part C: Design and Technology*, *6*(1), 1-16. 2018.

[3] Hatipoğlu, C., & Tunacan, T. "Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması", *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, 8(1), 430-445, 2021.

[4] Gündüz, M. Z., Resul, D. A. Ş. "Akıllı şebekelerde iletişim altyapısı ve siber güvenlik" *Journal of the Institute of Science and Technology*, *10*(2), 970-984, 2020.

[5] Benisha, R. B., Raja Ratna, S. "Design of intrusion detection and prevention in SCADA system for the detection of bias injection attacks." *Security and Communication Networks*, 108248.,2019.

[6] Khan, I. A., Pi, D., Khan, Z. U., Hussain, Y., Nawaz, A. "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems". *IEEE Access*, *7*, 89507-89521, 2019.

[7] Morris, T. H., Thornton, Z., Turnipseed, I. "Industrial control system simulation and data logging for intrusion detection system research." *7th annual southeastern cyber security summit*, 3-4, 2015.

[8] Gao, J., Gan, L., Buschendorf, F., Zhang, L., Liu, H., Li, P., Lu, T. (2020). "Omni SCADA intrusion detection using deep learning algorithms.", *IEEE Internet of Things Journal*, *8*(2), 951-961, 2020.

[9] Stewart, B., Rosa, L., Maglaras, L. A., Cruz, T. J., Ferrag, M. A., Simoes, P., Janicke, H. "A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes." *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 4(10), 1-11, 2017.

[10] Teixeira, M. A., Zolanvari, M., Khan, K. M., Jain, R., Meskin, N., "Flow-based intrusion detection algorithm for supervisory control and data acquisition systems: A real-time approach." *IET Cyber-Physical Systems: Theory & Applications*, 6(3), 178-191, 2021.

[11] Chu, A., Lai, Y., Liu, J. "Industrial control intrusion detection approach based on multiclassification GoogLeNet-LSTM model." *Security and Communication Networks*, 1-11, 2019.

[12] Kasongo, M. S., Sun, Y. "A Gated Recurrent Unit based Intrusion Detection for SCADA Networks." 6th International Conference on Computing, Communication and Security (ICCCS), 1-6, 2021.

[13] Pan, S., Morris, T., Adhikari, U. "Developing a hybrid intrusion detection system using data mining

for power systems" *IEEE Transactions on Smart Grid*, *6*(6), 3104-3113, 2015.

[14] Pan, S., Morris, T., Adhikari, U., "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data." *IEEE Transactions on Industrial Informatics*, *11*(3), 650-662, 2015.

[15] Zhang, H., Huang, L., Wu, C. Q., Li, Z. "An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset" *Computer Networks*, *177*, 107315, 2020.

[16] Karamollaoğlu H., Yücedağ İ., Doğru İ.A., "Saldırı Tespit Sistemlerinde Sınıf Dengesizliği Problemi", *International Conference on Engineering and Applied Natural Sciences*,1283-1288, 2022.

[17] Jafer, S. H. "Optimize network intrusion detection system based on PCA feature extraction and three naïve bayes classifiers." *Journal of Physics: Conference Series*, 2322(1), 1-12, 2022.

[18] Vinayakumar, R., Soman, K. P., Poornachandran, P. "Applying convolutional neural network for network intrusion detection." *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 1222-1228, 2017.