T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İKLİMLENDİRME SİSTEMLERİ ÜZERİNDE MAKİNE ÖĞRENMESİ İLE ANOMALİ TESPİTİ

YÜKSEK LİSANS TEZİ

Refik KİBAR

Bilgisayar Mühendisliği Anabilim Dalı

TEMMUZ 2023

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İKLİMLENDİRME SİSTEMLERİ ÜZERİNDE MAKİNE ÖĞRENMESİ İLE ANOMALİ TESPİTİ

YÜKSEK LİSANS TEZİ

Refik KİBAR

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Muhammed Fatih ADAK

Ortak Danışman: Dr. Öğr. Üyesi Kevser OVAZ AKPINAR

TEMMUZ 2023

Refik Kibar tarafından hazırlanan "İKLİMLENDİRME SİSTEMLERİ ÜZERİNDE MAKİNE ÖĞRENMESİ İLE ANOMALİ TESPİTİ" adlı tez çalışması 06.07.2023 tarihinde aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı :	**Dr. Öğr. Üyesi** Sakarya Üniversitesi	.....
Jüri Üyesi :	**Dr. Öğr. Üyesi** Rochester Teknoloji Üniversitesi Dubai	.....
Jüri Üyesi :	**Dr. Öğr. Üyesi** Sakarya Üniversitesi	.....
Jüri Üyesi :	**Dr. Öğr. Üyesi** Kırıkkale Üniversitesi	.....
Jüri Üyesi :	**Dr. Öğr. Üyesi** Ankara Sosyal Bilimler Üniversitesi	.....

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum "İKLİMLENDİRME SİSTEMLERİ ÜZERİNDE MAKİNE ÖĞRENMESİ İLE ANOMALİ TESPİTİ" başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

(05/06/2023).

Refik KİBAR

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteklerini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen ve mesai kavramı gözetmeden bu çalışmanın her anında yanımda olan değerli danışman hocalarım Dr. Öğr. Üyesi Muhammed Fatih ADAK'a ve Dr. Öğr. Üyesi Kevser OVAZ AKPINAR'a teşekkürlerimi sunarım.

Lisans ve yüksek lisans eğitimim süresince yardımlarını esirgemeyen Sakarya Üniversitesi Bilgisayar Mühendisliği Bölüm hocalarıma teşekkür ederim.

Anlayış ve yardımlarını esirgemeyen mesai arkadaşlarıma ve teşvikleriyle beni bu yolda yalnız bırakmayan değerli eşime ve aileme teşekkür ederim.

Ayrıca bu çalışmanın maddi açıdan desteklenmesine olanak sağlayan Sakarya Üniversitesi Bilimsel Araştırma Projeleri (BAP) Komisyon Başkanlığına (Proje No: 2023-19-43-16) teşekkür ederim.

Refik KİBAR

İÇİNDEKİLER

Sayfa

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ v
TEŞEKKÜR vii
İÇİNDEKİLER ix
KISALTMALAR xi
ŞEKİL LİSTESİ xiii
TABLO LİSTESİ xv
ÖZET xvii
SUMMARY xix
1. GİRİŞ 1
2. LİTERATÜR TARAMASI 5
2.1. HVAC Sistemine Ait Verisetlerinde Yapılan Çalışmalar 5
2.2. Kritik Altyapılarda Makine Öğrenmesi İle Anomali Tespit Çalışmaları 14
3. MATERYAL VE YÖNTEM 19
3.1. Makine Öğrenmesi 19
3.1.1. Denetimli öğrenme 20
3.1.2. Denetimsiz öğrenme 21
3.2. Anomali Tespiti 21
3.3. Zaman Serileri 23
3.4. Zaman Serilerinde Anomali Algılama Taksonomisi 24
3.4.1. Giriş verileri 24
3.4.2. Anomali türleri 25
3.4.2.1. Nokta anomaliler 25
3.4.2.2. Bağlamsal anomaliler 25
3.4.2.3. Toplu anomaliler 25
3.4.3. Yöntemin doğası 26
3.5. K-Ortalamalar 26
3.6. Ağaç Temelli Modeller 28
3.6.1. Karar ağaçları 28
3.6.2. Torbalama 29
3.6.3. Rastgele orman 30
3.6.4. Boosting 30
3.6.4.1. AdaBoost 30
3.6.4.2. Gradyan yükseltme makineleri 31
3.7. Hata Ölçüm Parametreleri 39
3.7.1. Belirleme katsayısı 39
3.7.2. Mean squared error (MSE) 39
3.7.3. Root mean squared error (RMSE) 39
3.7.4. Mean absolute error (MAE) 40
3.7.5. Mean absolute percentage error (MAPE) 40
3.8. Karışıklık Matrisi 40
3.8.1. Doğruluk 40
3.8.2. Kesinlik 41

3.8.3. Duyarlık 41
3.8.4. F ölçütü 41
3.8.5. ROC ve AUC 41
4. UYGULAMA 43
4.1. HVAC Sistemine Ait Veri Seti 43
4.2. Scikit Learn 44
4.3. Geliştirilen Uygulama 46
4.4. Kullanılan Makine Öğrenmesi Yöntemleri Ve Parametreler 47
4.5. Geliştirilen Model Ve Parametreleri 52
4.6. Web Tabanlı Anomali Tespit Uygulaması 57
5. SONUÇLAR VE ÖNERİLER 59
KAYNAKLAR 61
EKLER 71
ÖZGEÇMİŞ 75

KISALTMALAR

AUC :Area Under The Curve
BMS :Bina Yönetim Sistemleri
BSD :Berkeley Software Distribution
BT :Bagging Tree
CB :Catboost
CFD :Computational fluid dynamics
CPU :Merkezi İşlemci Birimi
DT :Decision Trees
DTR :Decision Tree Regressor
DVM :Destek Vektör Makinesi
EFB :Exclusive Feature Bundling
F1 :F-Ölçütü
FN :False Negatif
FP :False Pozitif
FTP :File Transfer Protocol
GBDT :Gradient Boosted Decision Trees
GBM :Gradient Boosting Machine
GBR :Gradient Boosting Regresör
GBRT :Gradient Boosting Regression Trees
GMM :Gaussian Mixture Models
GOSS :Gradient-Based One- Side Sampling
HTTP :Hyper Text Transfer Protocol
IEEE :Institute of Electrical and Electronics Engineers
IF :Isolation Forest
IoT :Nesnelerin İnterneti
HVAC :Heating, Ventilation And Air Conditioning
KNN :K-Nearest Neighbor
KNR :K-Neighbors Regressor
LIBLINEAR :Library For Large Linear Classification
LIGHTGBM :Light Gradient Boosting Machine

LR :Linearregression

MAE :Mean Absolute Error

MAPE :Mean Absolute Percentage Error

MDP :Markov Decision Process

ML :Machine Learning

MSE :Mean Square Error

NN :Neural Network

PCA :Principal Component Analysis

POSIX :Portable Operating System Interface For Unix

PRE :Precision

PYBRAIN :Python-Based Reinforcement Learning, Artificial Intelligence And Neural Network Library

PYMVPA :Multivariate Pattern Analysis In Python

RF :Random Forest

RFR :Random Forest Regressor

RMSE :Root Mean Squared Error

RNN :Reccurrent Neural Network

ROC :Receiver Operating Characteristic

SCADA :Merkezi denetleme kontrol ve veri toplama

SMTP :Simple Mail Transfer Protocol

SSH :Secure Shell

SWAT :Güvenli Su Arıtma

TN :True Negatif

TP :True Pozitif

TPU :Total Power Using

TRNSYS :Transient System Simulation Tool

WEB :World Wide Web

XAI :Explainable Artificial Intelligence

XGBOOST :Extreme Gradient Boosting

ŞEKİL LİSTESİ

Sayfa

Şekil 3.1. Zaman serilerinde anomali..... 22
Şekil 3.2. Sınıflandırma yöntemi ile anomali tespiti..... 22
Şekil 3.3. Zaman serilerinde anomali tespit teknikleri..... 24
Şekil 4.1. Algoritmalara ait tahmin grafiği. 48
Şekil 4.2. Kullanılan modellerin anomalilere verdikleri tepkiler..... 50
Şekil 4.3. Gerçek anomali değerleri. 50
Şekil 4.4. Algoritmalar tarafından anomali olarak tespit edilen noktalar. 51
Şekil 4.5. Parametre değişikliklerine göre alınan sonuçlar. 53
Şekil 4.6. Geliştirilen GBR* modeline ait tahmin grafiği..... 55
Şekil 4.7. Karışıklık matrisi sonuçları GBR*. 55
Şekil 4.8. GBR* modelinin anomali olarak tespit ettiği noktalar. 56
Şekil 4.9. GBR* ve ideal ROC eğrisi..... 57
Şekil 4.10. Web tabanlı projeye ait giriş sayfası..... 57
Şekil 4.11. Web tabanlı projeye ait sonuç ekranı..... 58

TABLO LİSTESİ

Sayfa

Tablo 3.1. İki sınıf bir sınıflandırıcı için karışıklık matrisi. 41
Tablo 4.2. Veri kümesi 3'te enjekte edilen saldırıların listesi. 45
Tablo 4.3. Modellerin test setindeki hata ölçüm parametreleri sonuçları. 47
Tablo 4.4. Modellerin veri kümesi 3 üzerinde hata ölçüm parametreleri sonuçları.. 49
Tablo 4.5. F-ölçütüne göre modellerin sonuçları. 52
Tablo 4.6. Modellerin karışıklık matrisi sonuçları. 52
Tablo 4.7. GBR* modelinin ait sonuçlar ve karşılaştırılması..... 54
Tablo 4.8. Geliştirilen modelin F-ölçütüne göre sonuçları ve karşılaştırılması. 55
Tablo 4.9. Geliştirilen modelin karışıklık matrisi sonuçları ve karşılaştırılması..... 56

İKLİMLENDİRME SİSTEMLERİ ÜZERİNDE MAKİNE ÖĞRENMESİ İLE ANOMALİ TESPİTİ

ÖZET

Kredi kartı dolandırıcılığı, siber saldırılar, terörist faaliyetleri veya bir sistemin bozulması gibi kötü niyetli faaliyetler gibi çeşitli nedenlerle verilerde anormallikler meydana gelebilir, ancak tüm nedenlerin ortak özelliği analiz için ilgi çekici olmalarıdır. Anomalilerin ilginçliği veya gerçek yaşamla ilgili olması, anomali tespitinin önemli bir özelliğidir. Anomali tespiti konusunda birçok yöntem denenmiştir. Bu tezde ısıtma, havalandırma ve iklimlendirme (HVAC) sistemine ait çok değişkenli bir zaman serisindeki siber saldırıları tespitinde makine öğrenmesi yöntemleri kullanılarak performansları karşılaştırılmıştır.

Anomali tespitinde doğrusal regresyon, karar ağaçları, k-en yakın komşu, rastgele orman ve gradyan artırma modelleri kullanılmıştır. Erişime açık HVAC sistemine ait bir zaman serisi olmadığından simülasyon sonucu elde edilen bir veri seti üzerinde modeller eğitilmiştir. Eğitilen modellerin yine aynı sisteme ait içinde 16 farklı siber saldırıyı barındıran bir veriseti üzerinde test edilmiştir. Karşılaştırılan sonuçlarda doğrusal regresyon ve gradyan arttırma modelinin iyi sonuç verdiği fakat anomalilerin tespiti noktasında çok iyi olmadığı gözlemlenmiştir. Büyük verilerde oluşabilecek aşırı yüklemenin modeller üzerinde olumsuz bir etkisi vardır. Veri kümesine ait öz nitelik seçimi önem arz etmektedir. Seçilen niteliklerin veri kümesini temsil etmesi tümüyle temsil etmesi gerekmektedir. Öz nitelik seçiminde temel bileşen analizi veya farklı derin öğrenme teknikleri kullanılmıştır. Korelasyonel ilişkide bu yöntemlerden biridir. Çıkış parametresi ile giriş parametreleri arasındaki ilişki incelenebileceği gibi çok değişkenli zaman serilerinde giriş parametreleri arasındaki ilişkide incelenebilir. Bu çalışmada giriş parametrelerinin birbirleriyle olan korelasyonel ilişkisi incelemiştir. +0,95 ve -0,95 ten yüksek ilişki gösteren değişkenler indirgenerek modeller tekrar eğitilmiştir. Siber saldırıları barındıran veri kümesi üzerinde test edilen algoritmaların sonuçları karışıklık matrisi ile karşılaştırılmıştır.

Sonuç olarak, GBR modelinin doğruluğunun kayda değer bir şekilde yükseldiği ve başarılı tespitler gerçekleştirdiği görülmüştür. Doğruluk değeri 0,64'ten 0,996'ya yükselmiş ve aynı zamanda modelin tahmin sonuçlarındaki hata değeri azalmıştır. Bu yaklaşım ile büyük verilerin özelliği göz önüne alınarak zaman serilerinde parametrelerin azaltılmasıyla doğruluğunun arttırılabileceği anlaşılmaktadır. Gelecek çalışmalarda farklı HVAC sistemlere ait veri setleri üzerinde çalışmalar yapılarak daha genel bir ifadeye ulaşılabileceği gibi farklı yöntemler ile parametreler azaltılıp makine öğrenmesi yöntemlerinin performansı karşılaştırılabilir. Ayrıca Django yazılım dili ile geliştirilen web sayfası ile gerçek zamanlı uygulamalara model olarak bir tasarım gerçekleştirilmiştir. Bu çalışma Django ile web tabanlı anomali tespiti için performans değerlendirme çalışmalarına örnek teşkil edilebilir. Farklı veri setleri üzerindeki analiz sonuçları ve işlem süreleri karşılaştırılabilir. Bu sayede, anomali tespit sistemlerinin etkinliğini ve ölçeklenebilirliğini değerlendirmeye yardımcı olacaktır.

ANOMALY DETECTION WITH MACHINE LEARNING ON AIR CONDITIONING SYSTEMS

SUMMARY

Anomalies in data can occur for a variety of reasons, such as credit card fraud, cyberattacks, terrorist activities, or malicious activities such as the disruption of a system, but the common feature of all causes is that they are of interest for analysis. The interestingness of anomalies or their relevance to real life is an important feature of anomaly detection. Anomaly refers to a situation that is normally unexpected or non-ordinary. For example, abnormal network traffic in a network, abnormal production data in a factory, or suspicious transactions in a financial system can be considered anomalies.

Anomaly detection is useful in many sectors. For example, it can be used in areas such as network security, financial services, manufacturing, healthcare, and others. Anomaly detection provides the following important advantages such as early diagnosis: Anomaly detection can identify problems in advance by detecting deviations from normal at an early stage. For example, detecting abnormal activity in a network can make a cyber attack noticeable before it starts. Efficiency and cost savings: Anomaly detection can provide efficiency and productivity in data-driven processes. While manually detecting abnormal situations can often be time-consuming and costly, machine learning models can quickly identify abnormal data and focus on problem areas. Fraud detection: Anomaly detection has a significant role in financial services and in the fight against fraud. For example, machine learning models can be used to detect credit card fraud or fraud attempts. Improved security: Anomaly detection plays an important role in network security and the fight against cyber threats. Detecting abnormal network traffic or malware activity allows us to quickly detect vulnerabilities and strengthen protection measures.

Machine learning for anomaly detection involves a variety of techniques used to learn normal behavior and then evaluate how abnormal a particular data point is. Learning-based methods allow the model to get better over time and produce more precise results. Many methods have been tried to detect anomalies. Accurate and fast anomaly detection is very important to prevent negative situations that will occur at the end of the system and process. The importance of the situation increases even more when critical infrastructures that such anomalies will know about or that are targeted by cyber attacks are targeted. Critical infrastructure; are large systems that contain subsystems that may cause loss of life and property, great and irreparable economic damage, personal and national security vulnerability and deterioration of public order when the characteristics, confidentiality, integrity or accessibility of the information they process are impaired.

However, with the developments in the technologies used, the importance of the security of building management systems (BMS) has increased. Since the Heating, Ventilation and Air Conditioning (HVAC) system in buildings accounts for about 40% of total energy consumption, threats targeting the HVAC system can be quite serious

and costly. Therefore, in this thesis study, their performances were compared using machine learning methods in detecting cyber attacks in a multivariate time series of heating, ventilation and air conditioning (HVAC) system. For this study, the data set of a 12-zone HVAC system collected from a simulation model using this thesis transient system was used due to the limitations in accessing a real HVAC system and the lack of general labeled data sets to investigate the cybersecurity of HVAC systems.

In the study, the training was carried out on the jupyter notebook version 6.5.2 using the gradient increase model. The model created using Visual Studio Code 17.5 was imported into the project. The system features Intel Core i7-10750H CPU 2.60GHz 2.59 GHz processor and nVIDIA GeForce GTX1650 Ti 4GB GDDR6 128-Bit DX12 graphics card. The model was implemented with Python version 3.9.15. SQLiteStudio 3.4.4 was used.

Linear regression, decision trees, k-nearest neighbor, random forest and gradient augmentation models were used for anomaly detection. Detailed comparisons and results of the models are given in Chapter 4. The trained models were tested on a database containing 16 different cyber-attacks belonging to the same system. These 16 different cyber-attacks can be evaluated in 4 different groups. Changing the set points of the control system, Falsifying sensor measurements by freezing their values or creating a bias, Falsifying control signals by freezing their values or creating a bias, Changing command signals to components. In the compared results, it was observed that the linear regression and gradient increase model showed good results, but the detection point of the anomalies was not very good. The normal behavior of anomalies is of great importance in this regard.

The overload that may occur in big data has a negative effect on the models. Attribute selection of the dataset is important. The selected attributes must fully represent the dataset. Basic component analysis or different deep learning techniques were used in the selection of attributes. Correlational relationship is one of these methods.

Correlational relationship refers to the relationship between variables in the data set. If a dataset contains a large number of input variables, high correlations can be found between these variables. In this case, the reduction of input variables or feature selection provides significant advantages over the dataset. Calculation Efficiency: Fewer input variables can reduce the calculation time of analysis and modeling operations. If there are high correlations between the variables in the data set, most of these variables carry the same information and there is no need to process repeated information in the analysis. Model Simplicity: Working with a small number of input variables increases the model's intelligibility and reduces the risk of overfitting. Complex models often underperform due to the presence of unnecessary or related variables. Feature selection makes the model simpler and more generalizable. Reduced Noise Effect: The relationship between correlated variables can reduce the noise effect on input variables. Variables that are not correlated or have a low correlation can adversely affect the performance of the model and cause misleading results. Feature selection helps to achieve more reliable results by reducing the noise impact. Generalizability: A small number of input variables increases the generalizability of the model. When the model is trained on a limited number of variables, it can better adapt to different data samples or new datasets. This allows the model to find a more general application area.

Especially in large datasets, reducing input variables with unnecessary or high correlation can improve the performance of the model and provide more efficient

analyses. In the light of this information, the relationship between the output parameter and the input parameters can be examined, as well as the relationship between the input parameters in multivariate time series. In this study, the correlational relationship of input parameters with each other was examined. Models were retrained by reducing variables with a higher relationship than +0.95 and -0.95. As a result of the operations, 30 input parameters were used by subtracting input variables that had no effect on the output value and had similar effects. The results of the algorithms tested on the dataset containing cyber attacks were compared with the confusion matrix. The confusion matrix is a metric table used to evaluate the performance of a model in classification problems. It is a commonly used tool in machine learning and data mining. The confusion matrix allows us to calculate performance measures such as accuracy, precision, recall, and F1 score by comparing the actual class labels with the predicted class labels of the model.

As a result, it was observed that the accuracy of the GBR model increased significantly and made successful determinations. A total of 591 data points, consisting of 351 normal and 240 anomaly instances, have been labeled for a time series. While all 351 normal data points were correctly predicted, 238 out of the 240 anomaly values were successfully detected. With these results, the accuracy value increased from 0.64 to 0.996, and at the same time the error value in the prediction results of the model decreased. With this approach, considering the characteristics of big data, it is understood that its accuracy can be increased by reducing the parameters in time series. Machine learning and anomaly detection provide significant benefits in many sectors such as security, efficiency and fraud detection. It is an effective tool for detecting abnormal situations early, responding quickly to problems, and providing a safer environment. In future studies, a more general statement can be reached by studying the data sets of different HVAC systems, and the performance of machine learning methods can be compared by reducing the parameters with different methods.

In addition, a design that will be a model for real-time applications was realized with the web page developed with the Django software language. Django provides a powerful infrastructure for web applications. Anomaly detection is a task that usually requires large amounts of data analysis and real-time processing. Django's rapid development features and flexible structure have been used to effectively manage the data flow and processing logic required for anomaly detection. And Django offers a scalable infrastructure for managing high-traffic web applications.

Anomaly detection is a task that requires analyzing large amounts of data in real time. Django's scalability features improve system performance and can effectively handle large data flows. The data in the time series are displayed according to the entered index value and applied to the developed GBR* model. Depending on the threshold value, the data of the time series are labeled as normal/anomaly and displayed. With the design realized, the model can be operated with the data read from the sensors and nodes. It is very important to detect the anomaly as soon as possible in order to prevent negative situations that may occur. The developed models can be used as a basis for wider studies with the changes to be made on the threshold value according to the tolerance value of the critical infrastructures to be applied. This study can be an example of performance evaluation studies for web-based anomaly detection with Django. Analysis results and processing times on different datasets can be compared. In this way, it will help to evaluate the effectiveness and scalability of anomaly detection systems.

1. GİRİŞ

Kullanılan teknolojilerdeki gelişmelerle birlikte Nesnelerin İnterneti'nin (IoT) üstel bir büyüme gerçekleşmiştir. Son zamanlarda yaşanan pek çok siber saldırı IoT özellikli olması buna dayanmaktadır. Saldırganlar kritik bir sistemi tehlikeye atmaya yönelik ilk adım olarak başlangıçta savunmasız IoT teknolojilerini kullanılır. IoT teknolojileri kritik altyapıların bir parçası olduğundan; endüstri, akıllı bina ve şebekeler, ulaşım ve tıbbi hizmetler gibi bazı sektörler için bu tür saldırılar oldukça önemlidir. Başlangıçta akıllı bina ve evler gibi nesnelerin internetinin son kullanıcı olduğu sistemler için olası tüm saldırı yolları incelenmediğinden HVAC sistemlerde bu saldırılar ile karşı karşıyadırlar. Bu nedenle son yıllarda bina yönetim sistemlerinin (BMS) güvenliğinin önemi artmıştır. Akıllı binalar çağıyla birlikte telekomünikasyon, kullanıcı sistemleri, can güvenliği, bina otomasyonu, tesis yönetim sistemi gibi pek çok sistem tek çatı altında entegre edilmektedir. Akıllı binalar konseptinin neredeyse kaçınılmaz gibi görünmesinin başlıca iki ana nedeni vardır. İlk olarak, kullanıcı zamanın %90'ını iç mekanlarda geçirdiğinden, bir bina içindeki çalışanlardan yüksek performans alma ihtiyacı önemlidir [1]. İkincisi, bina toplam enerji tüketiminin yaklaşık %40'ını tüketir ve aynı zamanda sera gazı emisyonlarının da %30'undan sorumludur [2]. Bu yüzden HVAC sistemini hedef alan tehditler oldukça ciddi ve maliyetli olabilir.

Akıllı binalarda bina ısıtma talebi, yangın alarm sistemi, güvenlik sistemi vb. çeşitli bileşenleri kontrol etmek için bir BMS kullanılmaktadır. Kullanıcıların konforu en çok ısıtma, havalandırma ve iklimlendirme (HVAC) işletiminden etkilenir ve ayrıca bina çalışır durumdayken en yüksek enerji tüketimi kaynaklarından biri olarak kabul edilir. Bir HVAC sisteminin verimli çalışması, önemli ölçüde BMS'nin yanı sıra denetleyici kontrol ve veri toplama (SCADA) sistemine bağlıdır. Termal bileşenlerin (örn. kazanlar) çalışması BMS yardımıyla yönetilirken elektrikli bileşenlerin çalışması SCADA tarafından yönetilir. Ancak bu tür akıllı binaların kontrolü ve yönetimi, kapsamlı bir bilgi ve veri alışverişinin yanı sıra fiziksel ve siber sistemlerin entegrasyonunu da gerektiriyor. Bu entegrasyonla, akılı binalarda hem dijital (ilgili veriler) hem de doğal kaynakların (su veya enerji gibi) optimum paylaşımı konusunda

büyük endişe vardır [2]. Bu nedenle, bu tür akıllı binalar önümüzdeki yıllarda yüksek güvenlik açıkları ve siber saldırı riskine maruz kalacaktır.

Binalara entegre edilen bileşenlerin sayısındaki artış, BMS'nin çevrimiçi olarak daha erişilebilir hale gelmesine neden olur [6]. SCADA'nın internete bağlanmasındaki bu son gelişme, yeni bir sistemin eski sistemle entegrasyonuyla sonuçlanmış ve sistemin siber saldırılara daha fazla maruz kalmasına yol açmıştır. Yapılan literatür taraması sonucunda, sisteme gerçekleştirilen saldırının tespitinin yanı sıra saldırı esnasında tespit edilmesinin de oldukça zor olduğu söylenebilir. Kritik altyapıların olduğu bir çağda mevcut durumda olduğu gibi, en büyük endişe bir elektrik arızası ile siber saldırı arasında ayrım yapmaktır. Saldırı ve hata arasındaki fark oluşturulduktan sonra, bir sonraki ana görev siber saldırı türünü tespit etmektir. Siber saldırı tespit edildiğinde, sistem dayanıklılığını sürdürmek için farklı kontrol politikaları tetiklenmelidir.

Aykırı değer tespiti, birçok araştırmacı ve uygulayıcının ilgi alanı haline gelmiştir ve zaman serisi olarak tasarlanan veri setlerinde çeşitli yöntemler ile tespit edilebilmektedir. Aykırı değer tespiti, kredi kartı sahtekarlığı tespiti, siber güvenlikte izinsiz giriş tespiti veya endüstride hata teşhisi gibi çeşitli uygulama alanlarında incelenmiştir [7].

Sıralı zaman serisi verilerinde diğer verilere kıyasla farklı zorluklar ortaya koyar. Enerji altyapısı, sağlık hizmetleri ve otomasyonlar gibi birçok kritik uygulamada önemlidir. Bu nedenle ayrı ayrı incelememiz gerekir. Bağımlı sonuç değişkenine sahip zaman serilerine giriş parametreleri işlemleri mevcut sistemi örneklemesine dikkat ederek işlem yapılmalıdır. Büyük önem taşıyan bu zaman serilerin bir risk altında olmadığını söylemek imkansızdır. Zaman serisi verilerindeki aykırı değerlerin analizi, zaman içindeki anormal davranışları inceler [8]. Fox 1972 yılında bu konudaki ilk çalışmayı gerçekleştirmiştir. Tek değişkenli zaman serilerinde iki tip aykırı değer tespit etmiştir. Tip1: tek bir gözlemi etkileyen, tip2: belirli bir gözlemi ve kendinden sonraki gözlemi etkiyen. Sonrasında bu çalışma Tsay tarafından dört tip aykırı değere daha sonra ise Tsay ve arkadaşları tarafından çok değişkenli zaman serilerine genişletilmiştir. Bu zamana kadar literatürde birçok aykırı değer teriminin yanımı ve çok sayıda tespit yöntemi önerilmiştir. Fakat bu konu üzerinde henüz bir fikir birliği sağlanamamıştır [9]. Örneğin; aykırı değer, aykırı gözlem, anomaliler, uyumsuz gözlem, uyumsuzluklar, istisnalar, sapmalar, sürprizler, tuhaflıklar veya kirleticiler olarak adlandırılır.

Bu çalışmada, Bölüm 2.'de konuyla ilgili çalışmalar araştırılmış ve literatürdeki benzer çalışmalar ve yöntemler sunulmuştur. Çalışmanın Bölüm 3. kısmı bu çalışmada kullanılmış olan metotlar ile ilgili teorik bilgileri içermektedir. Ayrıca çalışmada kullanılan veri ile ilgili bilgiler verilmiştir. Bölüm 4.'de ise çalışmanın adımları uygulanmasına ve sonuçlarına yer verilmiştir. Bölüm 5. ise uygulanan yöntemler ile elde edilen sonuçların karşılaştırılmasına ve değerlendirilmesi yer verilmiştir.

2. LİTERATÜR TARAMASI

2.1. HVAC Sistemine Ait Verisetlerinde Yapılan Çalışmalar

HVAC sistemlerde performansı arttırmaya yönelik ve siber saldırı tespitinde birçok çalışma yapılmıştır. Sistem maliyetini azaltmaya yönelik ve bir saldırı sonucunda oluşan zararın önüne geçmek için yapılan çalışmalar oldukça önem arz etmektedir. Bu amaç doğrultusunda farklı metotlara dayanan birçok yöntem kullanılmıştır. Bu yöntemlerin birbirleri ile performans kıyaslaması yapılmasa da henüz ortak bir fikir birliği sağlanamamıştır. Gerçekleştirilen yöntemlerin birden fazla model üzerinde yapılacak testleri bu konu hakkında genellenebilir yargıya ulaşmamızı sağlayabilir.

Keliris ve arkadaşları saldırıları erken aşamalarda tespit edebilen yeni savunma mekanizmaları tasarlamak maksadıyla bir kıyaslama kimyasal sürecini incelemiş ve çeşitli saldırı vektörleri kategorilerini ve bunların donanım denetleyicileri üzerindeki pratik uygulanabilirliğini bir Donanım-İçinde-Döngü test yatağında sıralamışlardır. Sürece ilişkin kategorize edilmiş saldırıların gözlemlenen sonuçlarından ve tipik bozulmaların profilinden yararlanarak, kötü niyetli etkinliğin erken belirtileri olan anormallikleri tespit etmek için veriye dayalı bir yaklaşım sunmuşlardır. Yaklaşım destek vektör makinalarıyla güçlendirilmiştir [10]. Destek vektör makinaları regresyon ilişkilerinde kullanıldığı gibi sınıflandırma problemlerinde kullanılmaktadır. Bu bilgiyi destekleyecek sonuçlar almışlardır. Paridari ve arkadaşları Güvenlik analitiği kullanılarak bir saldırı tespit edildiğinde esnek bir politika uygulayan yeni bir enerji yönetim sistemi siber-fiziksel-güvenlik çerçevesi önermişlerdir. Bu çerçevede anomali değerleri tespit etmek için veri noktaları arasındaki fiziksel korelasyonların tanımlandığı ve ardından anomali değer yerine tahmini bir değer kullanılarak kontrol döngüsünün kapatıldığı enerji yönetim sistemi verileri tarafından yürütülür. Çerçeve gerçek bir enerji yönetim sistemleri sitesinin azaltılmış sipariş modeli kullanılarak test edilmiştir [11].

Philipa ve arkadaşları Tahmin hatasını ve tahmini varyansını, denetimsiz bir şekilde HVAC arızalarını tespit edebilen bir destek vektör makinesi yenilik detektörüne girdi olarak kullanmışlardır. Deney sonuçlarında standart yenilik tespitini geliştirdiğini

sunmuşlardır [12]. Bu çalışmada önerilen yöntemin farkı DVM'nin arıza tespitinde kullanılması ve denetimsiz şekilde gerçekleşmesidir. Paridari ve arkadaşları endüstriyel kontrol sistemlerinde saldırı tespiti için bir analitik aracı içeren ve bir saldırı tespit edildiğinde güvenilir, tahmine dayalı, saldırıya dirençli bir kontrol politikası yürüten yeni bir siber-fiziksel güvenlik çerçevesi önermişlerdir. Önerilen bu çerçeve halihazırda uygulanan endüstriyel kontrol sistemlerinde uyarlanabiliyor. Önerilen çerçevenin performansı, gerçek bir enerji yönetim sistemleri sitesinin azaltılmış sıralı modeli ve simüle edilmiş saldırıları kullanılarak değerlendirilmiştir [13]. Bu çalışmada bir önceki çalışmalarına göre hazır sistemlere uygulanabilir olması kullanışlılık açısından bir fark yaratmıştırlar. Valli ve arkadaşları BACnet protokolünü ayrıntılı olarak değerlendirerek geleneksel izinsiz giriş tespit yöntemleriyle tespit edilemeyen bir tehdidin nasıl hafifletilebileceğini sunmuşlardır [14]. Jones ve arkadaşları kamu ve özel Tesis ve bina otomasyon sistemi ağları arasında siber güvenli bir bağlantı sağlayabilen bir bina otomasyonu saldırı tespit sistemi geliştirmiş ve test etmişlerdir. Ağ trafiğini denetimsiz yapay sinir ağı modellerinden uyarlanabilir rezonans teorisi ile değerlendirerek özel ve genel ağlardaki normal trafik etkinliğini öğrenebilmiştir. Geliştirilen algoritma ara bağlantı cihazına yetkisiz erişim girişimlerini ve bina otomasyon sistemine yönelik kötü niyetli bir siber-fiziksel saldırıyı tespit etmek için kullanılmıştır [15]. Çalışmada tek bir yapay sinir ağı algoritması denendiğinden dolayı çeşitli algoritmalar ile test edilip ayrıntılı deney yapmaya ihtiyaç vardır. Yapılan farklı çalışmalar algoritmanın etkinliği üzerine daha genel bir yargıya izin verecektir.

Wang ve arkadaşlarının önerdiği yöntemin teşhis performansı, oluşturulan fiziksel kısıtlamaların yeterli nitelik ve niceliğine bağlıdır. Kısıtlı bir optimizasyon olarak formüle edilir ve tüm sensör düğümlerinde paralel olarak yürütülen bir ceza fonksiyonu ile merkezi olmayan bir algoritma tarafından çözülür [16]. Bu nedenle daha sağlam bir mekanizma geliştirilmelidir. Guirguis ve arkadaşları Siber-Fiziksel Sistemleri siber saldırılara karşı korumak ve kontrol bloklarıyla düzenlemek için BLOC adında bir zaman çerçevesi önermişlerdir. Bu çerçeve optimal bir rastgele seçim bulmasını sağlamak için oyun teorik tekniklerinden yararlanır ve Siber-Fiziksel Sistemlerini güvence altına alır. Durum bilgisi olmayan bloklar için bir Stackelberg oyun modeli ve durum bilgisi olanlar için bir Markov oyun modeli geliştirmişlerdir. Rasyonel düşmanlardan kaynaklanan en kötü durum hasarını en aza indirmeyi

amaçlayan modeli kapsamlı simülasyonlar ve bir HVAC sistemi için gerçek bir uygulama aracılığıyla doğrulamışlardır [17]. Siber saldırıların karmaşık hale gelmesi ve kontrol edilecek savunma mekanizmalarının büyük ölçüde spesifik duruma gelmesi problemleri çözmek için maliyeti arttırmaktadır. Yapılan çalışma en kötü durum senaryosu altında gerçekleştirildiği için başarısı oldukça dikkat çekicidir.

Patil ve arkadaşları normal durum, arıza durumu ve saldırı arasında ayrım yapmak için bir makine öğrenme algoritması önermişlerdir. Sınıflandırma için destek vektör makine algoritması kullanılmış ve karşılaştırmalı bir çalışma ile diğer makine öğrenme algoritmalarına olan üstünlüğü gösterilmiştir [18]. KNN, RF ve BT ile karşılaştırılan DVM algoritmasının sınıflandırma problemlerinde bir kez daha üstünlüğünü ortaya koymuştur. Bu karşılaştırmalar makine öğreniminin hatayı siber saldırılardan ayırmak için potansiyel bir araç olduğunu doğrular niteliktedir. Roy ve arkadaşları Otomatik üretim kontrolü sistemlerini hedef alan yanlış veri enjeksiyonu ve hizmet reddi saldırıları gibi olası siber saldırı düzenlerini tespit etmek ve azaltmak için bir yöntem geliştirilmişlerdir. Önerilen yöntem, siber saldırı tespit ve hafifletme platformu olarak adlandırılır ve saldırıların tanımlanması ve hafifletilmesi için alan kontrol hatasının tahmin edilen verilerini kullanır. Stratejinin etkinliği, titiz simülasyon sonuçları kullanılarak doğrulanmıştır [19]. BMS'nin operasyonları büyük ölçüde iletişim katmanı veya bir siber katman ile koordine edilir. Bu nedenle BMS siber saldırılara çok yatkındır ve bu BMS'deki ana bileşenlerin arızalanmasına yol açabilir. Bir diğer önemli husus ise herhangi bir siber saldırıdan bağımsız olarak sistemdeki elektrik arızalarıdır. Sheikh ve arkadaşları Çalışmada Boole Tanımlama Stratejisi ile elektrik arızasını ve saldırısını tanımlamaya odaklanmışlardır. Saldırının tanımlanmasından sonra destek vektör makine sınıflandırıcısını kullanarak örüntü tanıma ile saldırı türlerini analiz etmişlerdir. Sonuçlar, en bilinen iki siber saldırının modelini tanıyarak önerilen stratejilerin etkinliğini göstermektedir [20]. Novikova ve arkadaşları HVAC sistemlerin günlük çalışma modellerini oluşturmak ve sistemdeki siber saldırı faaliyetinin belirtileri olabilecek şüpheli sapmaları tespit edebilen RadViz görselleştirmesini önermişlerdir. Bu model analiz edilen parametrelerin değerlerindeki değişikliklerin vurgulanmasına izin verecek şekilde oluşturulmuş HVAC parametrelerinin matris tabanlı bir temsili ile desteklenir. Önerilen görselleştirme modellerinin ayırt edici özelliği, farklı veri kaynaklarından gelen verileri görüntüleme yeteneğidir. Önerilen yaklaşımın etkinliğini göstermek ve değerlendirmek için HVAC

sistemi ve erişim kontrol sistemi günlüklerini içeren VAST MiniChallenge-2 2016 veri setini kullanmışlardır [21]. Verilerin eş zamanlı olarak analiz edilmesi anormal durumların hareketlerini açıklamaya imkan sağlamaktadır. Xu ve arkadaşları bir HVAC sisteminin anomali tespiti ve dinamik enerji performansı değerlendirmesi için bir veri madenciliği tabanlı yöntem önermişlerdir. Bu yöntemde, önce tarihsel çalışma verilerinden anormal çalışma verilerini tespit etmek ve anormalliklerin olası nedenlerini belirlemek için bir DM teknolojisi kullanılır. Daha sonra, hataların neden olduğu belirlenen anormal enerji tüketimi verileri düzeltilir. Bu temelde, çok seviyeli bir dinamik enerji performansı ölçütü ve HVAC sistemi için bir dizi enerji performansı değerlendirme kuralı oluşturulmuştur. Son olarak, bir HVAC sisteminin gerçek zamanlı çalışma performansı değerlendirilir ve anormal enerji tüketiminin nedenleri birden fazla seviyede tanımlanır. Önerdikleri yöntemin etkinliği, karmaşık bir soğutma sistemine sahip ticari bir binanın bir vaka çalışmasında doğrulanmıştır [22]. Bu yöntem esnek ve genişletilebilirdir ve bir HVAC sisteminin enerji tüketimini tahmin etmek, sistemi tanılamak ve optimize etmek ve diğer amaçlara ulaşmak için gerçek ihtiyaçlara göre bileşenleri seçilebilir veya değiştirilebilir.

Novikova ve arkadaşları görüntü benzerliği analizine dayalı HVAC veri analizine bir yaklaşım sunmuşlardır. Bu yaklaşım her gün için HVAC verilerinin grafik sunumunu oluşturup ardından oluşturulan her görüntü için yapısal benzerlik indeksini hesaplayarak benzerliklerini değerlendirmektir. Yüksek düzeyde farklılığın karakterize edildiği günler anomali günler olarak kabul edilmiştir. Önerilen yaklaşımı test etmek için HVAC sisteminden günlükleri içeren VAST MiniChallenge-2 2016 veri setini kullanmışlardır [23]. Ayrıca Novikova ve arkadaşları gerçek zamanlı modda izleme için uygulanabilen HVAC sistem günlüklerinin analizine görselleştirme odaklı bir yaklaşım sunmuşlardır. Sistemin durumunun neredeyse değişmeden kaldığı zaman periyotlarını tanımlayarak ve ısı haritasını kullanarak HVAC parametrelerinin ortalama değerlerini görselleştirmeyi önermişlerdir. Bu önerme HVAC sistemindeki değişikliklere çekmenin yanı sıra yaşam ritmini tespit etmeye olanak tanımıştır. Yaklaşım, üç katlı binanın işleyişini açıklayan VAST MiniChallenge-2 2016 veri setinde bir uygulama ile göstermişlerdir [24]. Filus ve arkadaşları Nesnelerin İnterneti sistemlerindeki belirli türdeki Botnet saldırıları için hafif bir detektör oluşturmak üzere öğrenen yinelenen sinir ağının kullanımını ele almışlardır. Modelin küçük bir 12 nöronlu tekrarlayan mimariye dayalı düşük hesaplama maliyeti uç cihazlar için

oldukça dikkat çekicidir. Deneylerde RNN'in, hızlı, basitleştirilmiş bir gradyan iniş algoritması kullanılarak çevrim dışı olarak eğitilebildiğini ve bunun, yüzde birkaç yanlış alarm oranıyla %96 civarında yüksek algılama oranlarına yol açabileceğini göstermişlerdir [25]. Bu çalışma hesaplama maliyeti düşük tutmak amacıyla basit tutulduğundan dolayı birden çok saldırı biçimini aynı anda tespit edemediğinden bazı riskler taşımaktadır. Novikova ve arkadaşları HVAC verilerini analiz etmek için kullanılan üç görselleştirme modelinin laboratuvar kullanılabilirlik testinin sonuçlarını sunmuşlardır (matris tabanlı görselleştirme tekniği, doğrusal olmayan çok boyutlu görselleştirme tekniği RadViz ve zaman çizelgesi). Matris tabanlı görselleştirme ve RadViz görselleştirme, anormallik algılama sürecinde sıklıkla kullanılırken, zaman çizelgeleri operasyonel HVAC verilerini sunmanın geleneksel bir yoludur. Kullanılabilirlik testi ile bu görselleştirme tekniklerinin davranış modeli ve anormallik tanımlama görevlerindeki avantajlarını ve sınırlamalarını ortaya çıkarmışlardır [26]. Model laboratuvar çalışması üzerinde test edilmiştir. Gerçek zaman serileri üzerinde geleneksel karşılaştırma modelleri ile karşılaştırılması modelin etkinliği hakkında daha çok bilgi verebilir. Bina sakinlerinin konforunu korurken, HVAC'ın enerji tüketimini azaltabilen, enerji açısından verimli bir bina termal konfor kontrol stratejisi tasarlamak çok önemlidir. Bununla birlikte, böyle bir stratejinin uygulanması zordur, çünkü bir bina ortamındaki termal durum değişiklikleri çeşitli faktörlerden etkilenir. Bu etkileyen faktörler arasındaki ilişkilerin modellenmesi zordur ve farklı bina ortamlarında her zaman farklıdır. Bu zorluğun üstesinden gelmek için Gao ve arkadaşları, binalarda termal konfor kontrolü için derin takviye öğrenme tabanlı bir çerçeve olan DeepComfort'u önermişlerdir. Termal konfor kontrolünü, HVAC'ın enerji tüketimini ve bina sakinlerinin termal konforunu birlikte dikkate alarak bir maliyet minimizasyonu problemi olarak formüle etmişlerdir. Derin ileri beslemeli sinir ağı tabanlı bir yaklaşım tasarlayıp ardından optimum termal konfor kontrol politikasını öğrenmek için derin deterministik politika gradyanları tabanlı bir yaklaşım önermişlerdir. Deneysel sonuçlar, yaklaşımlarının termal konfor tahmini performansını %14,5 oranında artırabildiğini ve HVAC'ın enerji tüketimini %4,31 oranında azaltırken, bina sakinlerinin termal konforunu %13,6 oranında artırabildiğini göstermiştir [27].

Bir başka DVM destekli model de Dey ve arkadaşları tarafından geliştirilmiştir. HVAC terminal ünitesini tespit etmek ve bunları otomatik ve uzaktan teşhis etmek için

bir yöntem açıklamışlardır. Bu amaçla, çok büyük hacimli verileri işlemek için tipik bir büyük veri çerçevesi oluşturulmuşlardır. Binayı daha akıllı hale getirmeye yönelik otomatik bir arıza tespit ve teşhis sistemi oluşturmak için kategorik bilgilere dayalı Çok Sınıflı Destek Vektör Makinesi kullanılmışlardır ve kümeleme ve sınıflandırma sonuçlarının iyi bilinen ve yerleşik algoritmalarla karşılaştırmış ve istatistiksel ölçümlerle doğrulamışlardır [28]. Li ve Tong bina termal ortamının gerçek zamanlı kontrolü için hem derin öğrenme hem de model tahmin kontrol algoritmalarının avantajından yararlanmak maksadıyla kodlayıcı-kod çözücü tekrarlayan sinir ağını kullanan derin öğrenme tabanlı model tahmin kontrol çerçevesi geliştirmiştir. Ek olarak, iç hava akışı ve HVAC sistemleri arasındaki dinamik etkileşimi simüle etmek için, önerilen bina kontrol stratejisini değerlendirmek için HVAC simülatörü ve hesaplamalı akışkan dinamiği (CFD) modelini entegre eden bir ortak simülasyon platformu geliştirmişlerdir. Önerilen yöntemin doğrulanması için karışım havalandırmalı kapalı bir alan ve güneş radyasyonuna maruz kalan bir ofis odası içeren iki vaka çalışmasını kullanmışlardır. Deney sonuçlarında %4 ve %7 enerji tasarrufu elde etmişlerdir [29]. Hesaplama verimliliği zaman alan CFD simülasyonları nedeniyle sınırlıdır. Literatürdeki diğer tekrarlayan sinir ağı kullanan modellerde benzer sınırlar mevcuttur. Nöron sayısını arttırmak çözüm olsa da maliyet artışına sebep olmaktadır.

Sensör verilerindeki olumsuz değişiklikler, bina sakinlerinin konforunu bozabilir veya enerji tüketimini artırabilir. Sensör ölçümlerinin değişikliğini tespit etmek için çeşitli izinsiz giriş tespit sistemleri önerilmiştir. Ancak, bu yaklaşımlar ya yüksek bir yanlış alarm oranı gösterir ya da anormallikleri tespit etmekte başarısız olur ve HVAC kontrolünü veya bina sakinlerini savunmasız bir duruma sokar. Haque ve arkadaşları akıllı bina sensörü ölçümlerindeki anormalliği belirlemek için iki denetimsiz makine öğrenme tekniğini (otomatik kodlayıcı ve tek sınıf destek vektör makinesini) birleştiren yeni bir izinsiz giriş tespit tekniği önermişlerdir. Deneysel sonuçlarda modellerin ayrı ayrı performansına bakıldığında tatmin edici sonuçlar vermediği ispatlanmıştır. Her iki modelin avantajlarını birleştirilerek, mevcut akıllı bina saldırı tespit sistemlerine kıyasla yanlış pozitif ve yanlış negatif oranlarında önemli düşüşler sağlanmıştır. Önerilen izinsiz giriş tespit sistemini ticari doluluk veri seti üzerinde değerlendirmiş ve önerilen modelin %99,6 F1 puanı elde edebildiğini bulmuşlardır [30]. Chakraborty ve arkadaşları Endüstriyel IoT saldırılarını gerçek zamanlı olarak

doğru bir şekilde izlemek için Endüstriyel IoT sensör okumalarını kullanan bir makine öğrenimi yaklaşımı oluşturmuşlardır. Güvenli Su Arıtma (SWaT) sistemine yönelik laboratuvar kontrollü bir dizi saldırı kapsamında IoT sistem davranışını analiz etmiş ve verilerden özellikler çıkarmak için fonksiyonel şekil analizi kullanarak dalga formunun profilini yakalayabilen yeni bir erken tespit yöntemi geliştirmişlerdir. Geliştirilen model IoT saldırılarını tahmin etmede işlevsel ve işlevsel olmayan yöntemler arasında verimlilik-karmaşıklık dengesi olduğunu göstermiştir [31]. Gerçek zamanlı endüstriyel IoT saldırı tespiti ile ilgili literatürde eksiklik olduğundan bu çalışma önem taşımaktadır. Werth ve arkadaşları OpenPLC gibi modern araçlar ve platformlar kullanılarak, bir HVAC sistemi için bir denetleyicinin prototipinin yapılabileceğini ve olası siber saldırıları ve bunların çeşitli siber fiziksel sistemlerdeki etkilerini araştırmak ve keşfetmek için kullanılabileceğini göstermişlerdir ve deneysel sonuçlarda, bu çalışma, ayarları değiştirmeye yönelik bir enjeksiyon saldırısı ve sanal test yatağına kötü amaçlı bir merdiven mantığı yüklemesi ile bu uygulamaların nasıl tehlikeye girebileceğini sunmuşlardır [32]. Günümüzde IoT akıllı ortamlarında, HVAC kontrolörleri, akıllı sayaçlar, duman dedektörleri vb. gibi düzinelerce cihaz türü mevcuttur. IoT cihazlarının güvenlik koşulları, şu ana kadar yetersiz kalıyor. Zayıf konfigürasyonlara ve açık tasarımlar, bellek ve bilgi işlemsel kaynak kısıtlamaları, pratik saldırı koruma mekanizmalarının uygulanmasını son derece zorlaştırıyor. Ve şu anda üreticiler, ekstra özellikler için bellekten tasarruf etmek için basitleştirilmiş ışık protokolü sürümlerini kullanıyor. Bu tür sorunlardan ve güvenlik açıklarından yararlanıldığında, cihazların güvenliği aşılabilir ve bir bot yöneticisi tarafından ciddi DDoS saldırılarının başlatılabileceği botlara dönüştürülebilir. Sudharsan ve arkadaşları MCU tabanlı IoT cihazlarının ağlara veya herhangi bir harici koruma mekanizmasına bağlı olmadan IoT saldırılarını anında algılamasını sağlayan Edge2Guard (E2G) olarak adlandırılan saldırı algılama modelleri önermişlerdir. Değerlendirme sırasında, en iyi performans gösteren E2G modelleri, %100'e yakın algılama oranlarıyla on tür Mirai ve Bashlite kötü amaçlı yazılım algılayıp ve sınıflandırmıştır [33]. Şebeke etkileşimli verimli binalar yalnızca pasif tehditlere değil, aynı zamanda ağ tabanlı kontrol sistemlerinde başlatılan siber saldırılar gibi aktif tehditlere de maruz kalır. Fu ve Arkadaşları Şebeke etkileşimli verimli binalarda üzerindeki siber saldırıların sonuçlarını ölçmek için bir modelleme ve simülasyon çerçevesi önermişlerdir. Simülasyon sonuçları, farklı türdeki saldırıların bina sistemlerini farklı boyutlarda tehlikeye atabileceğini, ancak bir soğutma grubunun

uzaktan kumandası yoluyla yapılan saldırıların hem bina hizmeti hem de şebeke hizmeti dahil olmak üzere bir bina sisteminin işleyişi üzerinde en önemli sonuçları verdiğini göstermektedir. Bir siber saldırının bina sistemlerini hem saldırı sürecinde hem de saldırı sonrasında etkilediğinin belirtilmesi, bir siber saldırının sonuçlarının tam olarak değerlendirilmesi için her iki dönemin de dikkate alınması gerektiğini göstermektedir [34]. Xu ve arkadaşları veri yetersizliğini eğitmedeki zorluğun üstesinden gelmek için soyut fiziksel modelden yararlanan model destekli bir öğrenme yaklaşımı sunmuşlardır. Ayrıca hatalı sensör okumalarına karşı HVAC sistemleri oluşturmak için yeni bir öğrenme tabanlı sensör hatasına dayanıklı kontrol çerçevesi sunmuşlardır. Modellerin eğitimde yapay sinir bileşenler yer vermişlerdir [35]. Çalışmada enerji verimliliğini korurken çeşitli sensör arıza durumlarında bina sıcaklığı ihlallerini önemli ölçüde azaltılabileceğini sunmuşlardır. Saldırı türlerinden, Dinamik yük değiştirme saldırıları altında siber fiziksel sistemlerin saldırı tespiti ve yeniden yapılandırılması önem arz etmektedir. Su ve arkadaşlarını yaptıkları çalışmada, saldırının sistem üzerindeki etkisini araştırmak için iki savunmasız yükün aynı anda saldırıya uğradığını varsayılarak gözlemci tarafından üretilen artık sinyalle saldırı yeniden yapılandırmasını uygulamak için sağlam bir gözlemci tasarlanmıştır. Bundan sonra, eşiği kalıntı ile karşılaştırarak saldırı tespitini tamamlamak için bir saldırı tespit mantığı uygulamışlardır. Gerçek zamanlı simülasyon platformunu kullanarak saldırı tespiti ve yeniden yapılandırmanın fizibilitesini doğrulamak için üç jeneratör ve altı bara güç sistemi örnek olarak vermişlerdir [36].

Metodoloji açısından çoğu çalışma, yalnızca bilinen saldırıların veya hataların sınıflandırılmasına izin veren sınıflandırmaya odaklanır. Yeni saldırılar tespit edilebilse de yeni bir saldırı mevcut sınıflandırıcılardan birine zorlanarak yanlış teşhise yol açacağından doğru şekilde teşhis edilemez. Coshatt Arkadaşları anormallikleri tespit etmek ve teşhis etmek için kümelemeyi kullanmayı önermektedir. Spesifik olarak, kümeleme için iki boyutlu denetimsiz şekilciklerin kullanılmasını önerir. U-şekilleri, bir veri kümesinden otomatik olarak çıkarılabilen ayrımcı yeteneklere sahip kısa zaman serileridir. Bu çalışma, dinamik kümelemeyi u-şekilleriyle birleştiren iki aşamalı bir çalışmanın ilkidir. Bu uzun vadeli yaklaşımın avantajı, bir sistemin sistem kullanıcılarını daha sonra etiketlenebilecek yeni bir saldırı veya hata türü hakkında bilgilendirmesine izin verir. Böylece sistem yeni anormallikleri tanımlamayı öğrenebilir [37]. Ishikawa diyagramı, kuruluşların etki yaratan faktörleri bulmak için

kullandıkları önemli araçlardan biridir. Bununla birlikte, literatürde henüz diyagramın en uygun biçimini ve genel köşe taşlarını belirlenememiştir. Elyoussoufi ve arkadaşları yaratıcı problem çözme teorisi ile Ishikawa diyagramını entegre ederek sistemi etkileyen faktörleri belirlemek için bir model sunmuşlardır [38]. Literatürde incelenen yaklaşımların çoğunda, iletilen verilerin gizli dinleme saldırılarından korunması ve kötü amaçlı bütünlük saldırılarının tespiti genellikle ayrı ayrı gerçekleştirilmiştir. Jiang ve arkadaşları eş zamanlı olarak güvenli iletim ve saldırı tespiti ile başa çıkmak için kontrol seviyesinde uygulanabilen entegre bir veri güdümlü çerçeve önermişlerdir. Çerçevede, güvenli bir korelasyon tabanlı şifreleme/şifre çözme yaklaşımı ve bir güvenilirlik yargısı yaklaşımı önerilmiştir. Önerilen yaklaşımların etkinliğini ve performansını göstermek için simüle edilmiş iki alanlı frekans-yük kontrollü elektrik şebekesi sistemi üzerindeki değerlendirme sonuçları sağlanmıştır [39]. KNX, bir bina otomasyon sistemi için popüler bir iletişim protokolüdür. Ancak, güvenlik eksikliği nedeniyle çeşitli siber saldırılar ile karşı karşıyadır. Literatürde ilk kez KNX tabanlı bina otomasyon sistemine yanlış veri enjeksiyon saldırısını tespit etmek için Cash ve arkadaşları destek vektör makinası tabanlı bir tespit stratejisi tasarlamışlardır. Gerçek dünya verileri ile test edilen modelin yanlış veri saldırı tespiti noktasında verimliliğini doğrulamışlardır. Ayrıca simülasyon sonuçlarında yanlış veri enjeksiyon saldırısının güç tüketimi açısından bina otomasyon sistemi üzerinde büyük bir etkisi olduğunu göstermişlerdir [40]. Ayrıca bina otomasyon sistemine intranet üzerinden, hatta uzaktan internet üzerinden erişim sağlamak yaygın bir uygulama haline gelmiştir. Bina otomasyon sistemlerinin sınırlı siber güvenlik hususları ile tasarlanmıştır ve akıllı binalar artan erişilebilirlik ile siber saldırılara karşı savunmasız hale gelmiştir. Bu amaçla Li ve arkadaşları üç alt ortamdan oluşan döngü içinde donanım adında bina topluluğunu bilgilendirmek ve bina endüstrisine siber-fiziksel güvenlik teknolojisi transferini desteklemek için kullanılabilen bir model geliştirmiştir [41].

HVAC sistemlere yapılan saldırılar veya sistemde oluşan hata ve arızalardan dolayı performans kaybına, enerji israfına ve binada yaşayanlar arasında rahatsızlığa neden olur. Bu durumları önlemek için HVAC sistemlerindeki hataların otomatik ve hızlı bir şekilde tanımlanması gerekir. Arıza teşhisi ve tespiti teknikleri bu amaçlar için oldukça etkilidir. Maliyet etkinliği ve veri kullanımı açısından en iyi arıza teşhisi ve tespiti süreç geçmişine dayanmaktadır, yani sistemden okunan sensör verilerine. Borda ve arkadaşları çalışmalarında denetimli ve yarı denetimli modeller geliştirmiştir. Dış

ortam sıcaklığı ve nem dışında, bir HVAC sisteminin giriş parametrelerinde çok az dahili değişken vardır. Özellikler arasındaki doğrusal olmayan ilişkileri yakalayabildikleri ve kolayca optimize edilebildikleri için Yapay Sinir Ağlarını kullanmışlardır. Aldıkları sonuçlara göre en iyi denetimli model Ortalama Mutlak Hatası 15 dakikada 0,032 ve 30 dakikada 0,034 'tür. En iyi yarı denetimli modelin ise Dengeli Doğruluk Değeri %86'dır [42].

2.2. Kritik Altyapılarda Makine Öğrenmesi İle Anomali Tespit Çalışmaları

Anormal kalıplar, veri odaklı yaklaşımlar kullanılarak oluşturulan termal konfor modellerini saptırabilir. Wang ve arkadaşları bu sorunu ele almak için öznel termal konfor verilerindeki aykırı değerleri tespit etmek için stokastik tabanlı iki aşamalı bir çerçeve önerilmişlerdir. Anomali tespit tekniği, K-güzel bir komşu (KNN) yöntemini kullanarak benzer koşulların tanımlanmasını ve daha sonra çok değişkenli bir Gauss yaklaşımı yoluyla benzer termal koşullar altında sakinlerin oylarının farklılığını ölçmeyi içermiştir. Çerçeveyi ASHRAE Global Thermal Comfort Veritabanı I & II'deki aykırı değerleri tespit etmek için kullanmışlardır. Ve ortaya çıkan anomali içermeyen veri kümesi sağlam konfor modelini ortaya çıkarmıştır. Önerilen yöntemin, aykırı değerleri termal talepte bireyler arası farklılıklardan etkili bir şekilde ayırt ettiği kanıtlamışlardır. Önerilen anomali tespit çerçevesi farklı değişkenlere sahip sistemlere uygulanabilir özeliktedir. Böyle bir araç, otomatik bina HVAC sistemleri için doluluk duyarlı kontrollerin geliştirilmesinde kullanılmasını öngörmüşlerdir [43]. Geliştirilen model verisetlerine bağlı olarak hiper parametreler üzerindeki ayarlamalar ile anomali tespit sürecinin performansı arttırabilir. Modern akıllı elektrik şebekesi elektrik talebini ve tüketimini yönetmek için çok verimli bir seçimdir. Fakat çok sayıda güvenlik tehdidiyle karşı karşıyadır. Doğal ve insan yapımı olaylar sistemde anormalliklere sebep olur. Bu nedenle operatörün karar alması ve uygun şekilde yanıt verebilmesi için nedenlerin ve türlerin belirlenmesi önemlidir. Bu nedenle Wang ve arkadaşları örnek verileri en yakın komşunun sınıfına atamak, bir küme oluşturmak ve son olarak saldırı tespiti için KNN'yi kullanmışlardır [44]. Elde edilen sonuçlar sekiz farklı teknik ile karşılaştırılmış ve deneysel sonuçlar bu modelin %93,91'lik doğruluk oranına ve %93,6'lık tespit oranına ulaşabildiğini göstermektedir. Enerji tüketiminde anormallik tespiti, verimli enerji tasarrufu sistemleri geliştirmeye, toplam enerji harcamasını azaltmaya ve karbon emisyonlarını azaltmaya yönelik çok önemli bir

adımdır. Bu nedenle binalarda anormal tüketimi belirlemek için güçlü tekniklerin uygulanması ve bu bilgilerin son kullanıcılara ve yöneticilere sağlanması büyük önem taşımaktadır. Bu yüzden Himeur ve arkadaşları iki yeni şema önermişlerdir. İlki, tek sınıf destek vektör makinesine dayalı denetimsiz bir anormallik tespitidir. Burada anormallikler, açıklamalı verilere ihtiyaç duyulmadan ayıklanır. İkincisi mikro anlara dayalı denetimli bir anormallik tespitidir. Verilerin normal veya anormal olarak sınıflandırmak için geliştirilmiş bir K-en yakın komşu modeli tanıtılmıştır. Bu çerçevede üç farklı veri seti altında yaptıkları ampirik değerlendirme, yöntemin hem en yüksek anormallik tespit performansına hem de gerçek zamanlı işleme kabiliyetine diğer makine öğrenme yöntemlerine kıyasla oldukça düşük hesaplama maliyeti ile ulaştığını göstermektedir. Katar Üniversitesi enerji laboratuvarında toplanan gerçek dünya veri seti kullanılarak %99,71'e varan doğruluk ve %99,77 F1 puanı elde etmişlerdir [45]. Makine öğrenmesi yöntemleri sınıflandırma işlemlerinde oldukça başarılı sonuçlar vermiştir. Parizad ve arkadaşları bir güç sistemindeki siber saldırıları algılamak için durum değişkeni davranışında sapmaya yol açan işbirlikçi bir makine öğrenimi tabanlı çerçeve önermektedir. Algılama sürecinde en iyisini bulmak için üç farklı makine öğrenimi tabanlı yöntem kullanılıp karşılaştırılmıştır (IF, DVM, KNN). Çerçevede ilk aşamada ön işleme yapılır. İkinci aşamada, durum vektörlerinin örüntüleri özniteliklere aktarılır. Bu nedenle, çeşitli özellikleri bulmak için merkezi eğilim ölçüleri, değişkenlik, şekil ölçüleri ve konum ölçüleri dahil olmak üzere 24 istatistiksel özellik çıkarılır. Ardından, üçüncü aşamada, FDIA'daki en önemli özellikleri sıralamak ve bulmak için denetimli bir algoritma kullanılır. Dördüncü aşamada, özellik alanını azaltmak için denetimsiz bir boyutluluk azaltma tekniği (PCA) uygulanır. Beşinci ve son aşamada, tespit etmek için görselleştirme, sınıflandırma ve kümeleme tabanlı yöntemler geliştirilmiştir. Önerilen yöntemin etkinliği, IEEE 14-bus sistemine uygulanan New York Bağımsız Sistem Operatörü verileri üzerinde değerlendirilmiştir [46].

Kamu hizmeti sağlayıcılarının enerji hırsızlığı nedeniyle yılda milyarlarca dolar kaybedeceği tahmin ediliyor. Akıllı şebekelerin uygulanması teknik ve sosyal avantajlar sağlasa da akıllı şebekelerde konuşlandırılan akıllı sayaçlar, geleneksel mekanik sayaçlara kıyasla enerji hırsızları tarafından daha fazla saldırıya ve izinsiz ağ girişlerine karşı hassastır. Yip ve arkadaşları enerji hırsızlığı yapan tüketicileri belirlemek ve güç sistemi hesaplamalarını yanıltmak için kullanılan hatalı ekipmanı

bulmak için doğrusal regresyona dayalı LR tekniğini kullanmışlardır ve iki farklı algoritma geliştirmişlerdir [47]. Yine enerji hırsızlığı ile oluşacak arz talep dengesindeki sorunları ve şüpheli kullanıcıların belirlenmesi amacıyla Jindal ve ark., Jokar ve ark., ve Messinis ve arkadaşları; Yanlış Veri Enjeksiyon Saldırı tespitinde verileri saldırıya uğrayan ve normal olanlara göre sınıflandırmak için hiper düzlem sınırlarını kullanan destek vektör makinalarına ve karar ağaçlarına dayanan model sunmuşlardır [48-50]. Evrişimli sinir ağı özellik çıkarımda ve sınıflandırma sürecini otomatikleştiren yaygın bir tekniktir. Hasan ver arkadaşları enerji hırsızlığı konusunu yapay veri seti üzerinde incelemişlerdir. Akıllı veri şebekelerinde normal kullanıcı ve enerji hırsızlarının sınıflandırılmasında evrişimli sinir ağı tabanlı LSTM modelini oluşturmuşlardır. Oluşturan model veri seti üzerinde yüksek doğrulukla sınıflandırma yapabilmiştir [51].

Binalarda oda sıcaklığı kontrolü için Model Öngörülü Kontrol, binalarda enerji yönetimine yönelik etkili bir yaklaşımdır. Bununla birlikte, fiziksel modellerin geliştirilmesi ve sürdürülmesi, özellikle konut binaları için yaygın gerçek yaşam uygulaması için problemler oluşturabilir. Bünning ve arkadaşları gerçek hayattaki bir apartman dairesinde oda sıcaklığını kontrol etmek için afin fonksiyonlara ve dışbükey optimizasyona sahip Rastgele Orman tekniğine dayalı bir Veri Öngörülü Kontrol yaklaşımının bir uygulamasını sunmuşlardır. Geleneksel histerezis denetleyicisi ile karşılaştırıldığında, uygulanan yaklaşım, soğutma enerjisinden %24,9 tasarruf sağlarken, altı günlük bir deneyde konfor kısıtlaması ihlallerinin integralini %72,0 oranında azaltmış fakat daha uzun tahmin ufuklarına ihtiyaç duyulduğunda sınırlamalar göstermiştir [52]. Sistemler üzerinde tahmin ve sınıflandırma işlemlerinin doğruluğu ve genellenebilirliği, büyük ölçüde, siber saldırılara karşı çok hassas olan veri kalitesine bağlıdır. Yanlış veri enjeksiyonu saldırıları, mevcut operasyonel uygulamalar tarafından kolayca tespit edilemeyebilecek, sözde korunan verilerin büyük bir bölümünü kötü niyetli olarak değiştirebilecek ve böylece tahmin performansını bozarak güç sisteminde olumsuz sonuçlara yol açabilecek bir siber saldırı sınıfı oluşturur. Ahmadi ve arkadaşları izinsiz girişleri otomatik olarak tespit etmek ve böylece enerji tahmin sistemlerinin güvenilirliğini ve dayanıklılığını zenginleştirmek için yeni bir veri odaklı Yanlış veri enjeksiyonu saldırı tespit mekanizması önermişlerdir. Önerilen mekanizma, sistemin modellerini veya parametrelerini kullanmadan düşük hesaplama maliyeti ve yüksek ölçeklenebilirlik ile

doğru tespitler sağlayan çapraz doğrulama, en küçük kareler ve z skoru metriğine dayanmaktadır. Önerilen dedektörün etkinliği, altı temsili ağaç tabanlı rüzgâr gücü tahmin modeliyle desteklenir. Deneyler, girdi, çıktı ve girdi-çıktı verilerine enjekte edilen bozuk verilerin düzgün bir şekilde yerleştirildiğini ve kaldırıldığını, böylece nihai tahminlerin doğruluğunun ve genellenebilirliğinin geri kazanıldığını göstermektedir [53]. Makine öğrenmesi algoritmalarının yanında anomalilerin karmaşık, belirsiz ve zamana bağlı doğasını öğrenebildikleri için tekrarlayan sinir ağları da HVAC sistemlerde sistem arızalarını algılamak için kullanılmaktadır. Tekrarlayan sinir ağları ampirik doğası nedeniyle hesaplama açısından pahalı bir görev olan hiper parametre optimizasyonu araştırılmamıştır. Taheri ve arkadaşları arızalı ve normal şartlarda farklı derecelerdeki arızaları otomatik olarak tespit edebilen yedi adet tekrarlayan sinir ağı konfigürasyonu devreye almış ve ayarlamıştır. Ardından, önerilen tüm konfigürasyonları doğruluklarına ve eğitim hesaplama sürelerine göre optimize etmek ve karşılaştırmak için kapsamlı bir hiperparametre çalışması yapmışlardır. Önerilen modeli ile diğer iki gelişmiş veriye dayalı teknik, yani rastgele orman (RF) ve gradyan artırma (GB) arasında bir karşılaştırma yapmışlar ve tekrarlayan sinir ağı modelinin RF ve GB regresyonundan önemli bir farkla daha iyi performans göstermiştir [54]. Punmiya ve arkadaşları, Razavi ve arkadaşları; siber saldırıları tespit etmek için gradyan yükseltme ve Naive Bayes sınıflandırıcısını kullanmışlardır [55,56]. Khan ve arkadaşları HVAC saldırıları tarafından oluşturulan günlük verilerini kullanarak farklı güvenlik saldırılarını tespit etmek için makine öğrenimi ve açıklanabilir yapay zeka (XAI) kullanan proaktif, yorumlanabilir bir tahmin modeli önermişlerdir. DT, RF, GB, AB, LGBM, XGBoost ve CatBoost (CB) gibi çeşitli makine öğrenimi algoritmaları kullanılmış ayrıca özellik seçimi için FFS tekniğini kullanmışlardır. Veri dengesizliğini azaltmak için de SMOTE ve Tomeklink teknikleri karşılaştırılmış ve SMOTE tekniği ile seçilen özelliklerle en iyi sonuçları elde edilmiştir. Ampirik deneyler yapılmış ve sonuçlarda XGBoost sınıflandırıcısının 0.9999 AUC, 0.9998 doğruluk, 0.9996 Recall, 1.000 Precision ve 0.9998 F1 Score ile en iyi sonucu verdiğini göstermişlerdir. Önerilen çalışmanın sonuçları, IoT cihazlarına ve Endüstri 4.0'a yönelik siber güvenlik saldırılarını tahmin etmede makine öğreniminin etkinliğini doğrulamıştır [57]. Termal konfor modeli ve tahmini toplam güç kullanımı, HVAC sistemine karşı başlatılan kötü niyetli eylemlerin büyüklüğünü değerlendirmek için kullanılır. Elnour ve arkadaşları incelenen sistemin veri odaklı bir saldırı algılama stratejisini geliştirmek ve doğrulamak için izolasyon ormanı

kullanarak yarı denetimli bir yaklaşım geliştirmişlerdir. Önerilen yaklaşım, standart makine öğrenme yaklaşımlarıyla karşılaştırılmıştır. Yüksek güvenilirlik-düşük hesaplama maliyetine sahip bir dizi saldırı senaryosu için saldırı tespitinde tatmin edici sonuçlar vermiştir [58]. Bode ve arkadaşları, LR, kNN, CART, RF, NB, SVM, NN modellerini karşılaştırmışlardır. Ulusal Standartlar ve Teknoloji Enstitüsü tarafından sağlanan ve özel donanımlı bir hava-su ısı pompasında ölçülen tipik ısı pompası arızalarına ilişkin verileri içeren bir veri seti kullanmışlardır. Ulusal Standartlar ve Teknoloji Enstitüsü veri setindeki hataları tespit etmek için algoritmaları eğitmişler ve takılan anomali tespit algoritmalarına ait ölçüm verilerine aktarmışlardır. Eğitimli anomali tespit algoritmalarının Ulusal Standartlar ve Teknoloji Enstitüsü veri setinde çok iyi performans gösterdiğini, ancak gerçek dünya veri setinde kötü performans gösterdiğini sunmuşlardır. Anomali tespit algoritmalarının düşük performansının çeşitli nedenlerini belirlemiş ve hafifletici eylemler türetmişledir. Anomali tespit algoritmaları için büyük veri yaklaşımlarının, büyük veri miktarlarının basit bir şekilde toplanmasının ötesinde, özellikle meydana gelen hataların etiketlenmesi ve veri setinin eksiksizliği gibi çeşitli sorunlarla karşı karşıya olduğuna öngörmüşlerdir [59].

3. MATERYAL VE YÖNTEM

3.1. Makine Öğrenmesi

Makine öğrenmesi makinelere verileri nasıl daha verimli şekilde kullanacaklarını öğretmek için kullanılır. Makine öğrenmesinin amacı verilerden öğrenmektir. Makinelerin kendi kendine öğrenmesinin nasıl sağlanabileceği konusunda birçok çalışma yapılmıştır [60].

Makine öğrenmesi veri sorunlarını çözmek için farklı algoritmalara dayanır. Veri bilimcileri, bir sorunu çözmek için en iyi olan algoritmanın, her duruma uygulanamayacağını belirtmektedirler. Kullanılan algoritmanın türü çözülmek istenen problemin türüne, değişken sayısına, ona en uygun modelin türüne vb. bağlıdır [60]. Makine öğrenimi genellikle iki ana türe ayrılır.

Birinci makine öğrenme türü; tahmine dayalı veya denetimli öğrenme yaklaşımında amaç, etiketli giriş-çıkış üzerinden bir çıkarımda bulunmaktır.

$$D = \{(x_i, y_i)\}_{i=1}^{N} \tag{3.1}$$

Burada D eğitim seti, N eğitim örneklerinin sayısı olarak adlandırılır.

Çıkış veya sonuç değişkeninin değeri prensipte herhangi bir şey olabilir, ancak çoğu yöntem y_i'nin bazı sonlu kümelerden kategorik veya nominal bir değişken olduğunu varsayar. y_i kategorik olduğunda sorun sınıflandırma veya örüntü tanıma olarak, y_i gerçek değerli olduğunda sorun regresyon olarak tanımlanır. Sıralı regresyon olarak bilinen başka bir varyant, Y etiket uzayının A-F dereceleri gibi bazı doğal sıralamaya sahip olduğu durumlarda ortaya çıkar.

İkinci makine öğrenme türü; tanımlayıcı veya denetimsiz öğrenme yaklaşımıdır. Bu yöntemde ilginç örüntülerin bulunması amacıyla sadece giriş değişkenleri verilir.

$$D = \{(x_i)\}_{i=1}^{N} \tag{3.2}$$

Bu bazen bilgi keşfi olarak adlandırılır. Belirli bir x için y'nin tahminini gözlemlenen değerle karşılaştırabileceğimiz denetimli öğrenmenin aksine bize ne tür kalıpları

arayacağımız söylenmediğinden ve kullanılacak bariz bir hata ölçüsü olmadığından daha çok daha az iyi tanımlanmış bir problemlerdir.

Daha az kullanılan ve fazla yaygın olmayan üçüncü makine öğrenme türü; Takviyeli/Pekiştirmeli öğrenme yaklaşımıdır. Bu yöntemde ara sıra ödül veya ceza sinyalleri verildiğinde nasıl davranılacağını veya davranılmayacağını öğrenmek için yararlıdır. Takviyeli/Pekiştirmeli öğrenmeni temeli karar teorisine dayanmaktadır [61].

3.1.1. Denetimli öğrenme

Modelde eğitim verisetinde bulunan giriş değişkenleri ve bu giriş değişkenlerine bağlı etiketli çıktılar üzerine kurulur. Kurulan modeli doğrulayan öğrenme yöntemi denetimli öğrenme olarak adlandırılmaktadır. Denetimli öğrenme sınıflandırma ve regresyon olmak üzere iki başlığa ayrılır.

Regresyon yöntemi: Çıkış değişkeninin sayı olduğu verisetleri üzerindeki yapılan işlemler regresyon olarak adlandırılır. Bağımlı olan çıkış değişkeninin, bağımsız bir veya birden fazla değişken tarafından modellenmesi olarak açıklanabilir. Bağımsız değişkenlerin sahip olduğu katsayılar bağımlı değişkene etki düzeylerini ifade etmektedir. Sayısal bağımlı değişkenlerin tahmin edildiği problemler için regresyon yöntemi kullanılabilir. Regresyon yöntemi doğrusal ve doğrusal olmayan olmak üzere iki alt kategoride incelenebilir.

Doğrusal regresyon yöntemi sayısal tahminler kullanılan çok basit bir denetimli öğrenme yöntemidir. Bağımsız değişkenlerin katsayıları ile çarpılarak elde edilen sonuca sabit değişkenin eklenmesiyle sonuç hesaplanmaktadır. Çoklu doğrusal regresyonlarda bağımsız değişken sayıları farklılık gösterebilmektedir.

Doğrusal olmayan regresyon yöntemi bağımlı ve bağımsız değişkenler arasında belirgin bir ilişki olmadığı durumlarda tercih edilen bir yöntemdir [62].

Sınıflandırma Yöntemi: Çıkış değişkeninin nitel/kategorik değişken olduğu verisetlerinde bu nitel durumun tahmin edildiği yöntemler sınıflandırma yöntemleri olarak adlandırılır. Bu yöntem ile bilinmeyen bir değişkenin, bilinen sınıflardan hangisine ait olduğunu bulmayı amaçlamaktadır [63]. Sınıflandırma yöntemi doğrusal ve doğrusal olmayan olmak üzere iki alt kategoride açıklanabilir.

Doğrusal sınıflandırma yöntemi: İki veya çok boyutlu düzlemde verisetinde benzer özellik gösteren örnekleri ayrıştırmak amacıyla kullanılan yöntemlerdir. Sınıflandırılan örneklerin birbirlerine uzaklıkları doğrusal olduğu durumlarda kullanılır.

Doğrusal olmayan sınıflandırma yöntemi: Doğrusal olarak ayrılamayan verileri sınıflandırmak için kullanılan yöntemdir. Bu yöntemde sınıflandırma sınırlarının herhangi bir şekil sınırı yoktur [63].

3.1.2. Denetimsiz öğrenme

Etiketin olmadığı veya kaç adet olduğunun bilinmediği verisetlerinde kullanılan modeldir. Örnekler üzerinde benzerliklerinin veya farklılıklarının nedenini belirlemek amacı üzerine inşa edilir. İlk kez Tryon tarafından kullanılan kümeleme en yaygın denetimsiz öğrenme yöntemidir [64].

Veriyi sınıflara veya kümelere ayırma işlemi sırasında değişkenler arasında herhangi bir bağımlılık durumu bulunmayan veri setlerinde anlamlı sonuçlar üretilebilir. Her küme içerisindeki gözlemler kendi içlerinde benzerlik gösterirken diğer kümelere ait farklı özellikler barındırmaktadır [62].

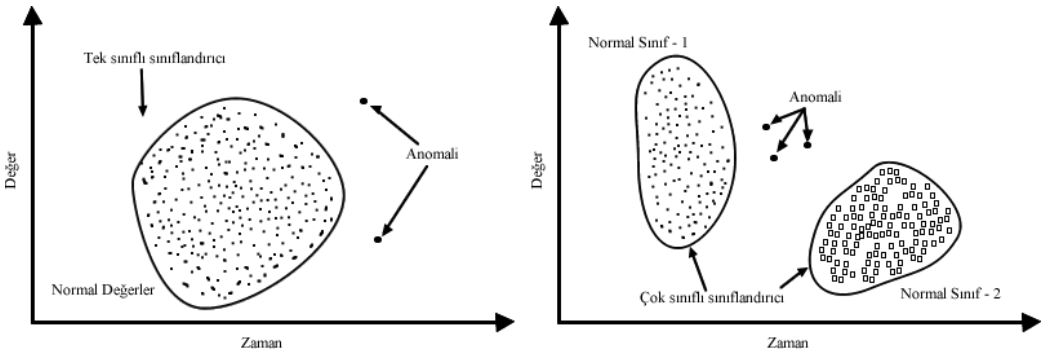
Kümeleme yöntemleri ile verisetinde yer alan değişkenlerin benzerlik belirleme işlemleri uzaklık-yakınlık, yoğunluk ve komşuluk gibi durumlar göz önüne alınsa da çoğu gruplama işlemi uzaklık-yakınlık hesaplamaları ile elde edilen uzaklık ölçütü değeri kullanılır [63].

3.2. Anomali Tespiti

Anormallikler, iyi tanımlanmış bir normal davranış kavramına uymayan verilerdeki kalıplardır. Anomali tespiti; kredi kartları, sigorta veya sağlık hizmetleri için dolandırıcılık tespiti, siber güvenlik için izinsiz giriş tespiti, güvenlik açısından kritik sistemlerde arıza tespiti ve düşman faaliyetleri için askeri gözetim gibi çok çeşitli uygulamalarda geniş kullanım alanı bulmaktadır. Örnek bir zaman serisi üzerindeki anomali görüntüsüne Şekil 3.1’de ki şekilde yer verilmiştir.

Şekil 3.1. Zaman serilerinde anomali.

Anormallik tespitinin önemi, verilerdeki anormalliklerin çok çeşitli uygulama alanlarında önemli ve genellikle kritik bilgiler üzerinde gerçekleşmesinden kaynaklanmaktadır. Örneğin, bir bilgisayar ağındaki anormal bir trafik modeli, saldırıya uğramış bir bilgisayarın hassas verilerini yetkisiz bir hedefe gönderdiği anlamına gelebilir. Anormal bir MRI görüntüsü, kötü huylu tümörlerin varlığını gösterebilir. Kredi kartı işlem verilerindeki anormallikler, kredi kartı veya kimlik hırsızlığına işaret edebilir veya bir uzay aracı sensöründen gelen anormal okumalar, uzay aracının bazı bileşenlerinde bir arızaya işaret edebilir. Bütün nedenlerin ortak özelliği analiz için ilgi çekici olmalarıdır. Anomalilerin ilginçliği veya gerçek yaşamla ilgili olması, anomali tespitinin önemli bir özelliğidir [65]. Tek ve çok sınıflı sınıflandırma yöntemi ile oluşabilecek anomali durumlarına Şekil 3.2'de yer verilmiştir.



Şekil 3.2. Sınıflandırma yöntemi ile anomali tespiti.

Basit bir anomali tespit yaklaşımı normal davranışı temsil eden bir küme belirlemek ve veriseti içerisinde bu kümeye ait olmayan gözlemlerin anomali olarak adlandırmaktır. Ancak birkaç neden bu basit tanımlamayı zorlaştırır:

- Her normal gözlemi kapsayan normal bir küme tanımlamak zordur ve normal - anormal davranışlar arasındaki sınır genellikle kesin değildir. Bu nedenle sınıra yakın bir anormal bir gözlem normal olabileceği gibi bunun tersi de mümkündür.
- Anomaliler genelde kötü niyetli kullanıcılar tarafından gerçekleştirildiğinden, düşmanlar genellikle anomali gözlemlerin normal görünmesini sağlamaya çalışırlar ve bu durum normal davranış kümesini tanımlamayı daha zor hale getirir.
- Pek çok alanda normal davranış gelişmeye devam ediyor ve mevcut bir normal davranış kavramı gelecekte yeterince temsil edici olmayabilir.
- Anomali kavramı farklı uygulama alanları için benzerlik göstermeyebilir. Örneğin tıp alanında normalden küçük bir sapma anomali olarak adlandırılabilirken bu durum borsa alanında normal olarak kabul edilebilir. Bu durumdan dolayı bir alanda geliştirilen tekniği diğerine uygulamak kolay değildir.
- Anomali tespit teknikleri tarafından kullanılan modellerin eğitimi/doğrulanması için etiketlenmiş verilerin bulunması genellikle önemli bir sorundur.
- Genellikle veriler, gerçek anormalliklere benzer olma eğiliminde olan ve bu nedenle ayırt edilmesi ve ortadan kaldırılması zor olan gürültü içerir.

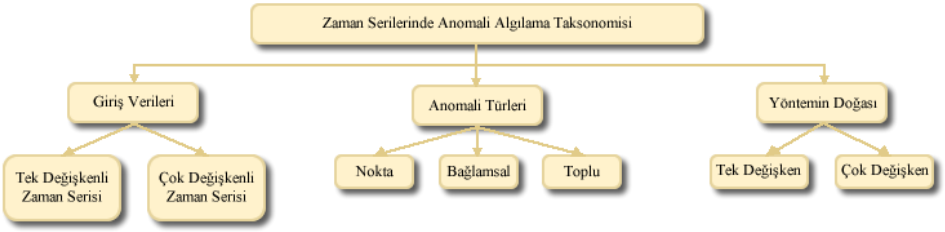
Bu zorluklar nedeniyle, en genel şekliyle anomali tespit probleminin çözülmesi kolay değildir. Aslında, mevcut anormallik tespit tekniklerinin çoğu, sorunun belirli bir formülasyonunu çözer. Formülasyon, verilerin doğası, etiketlenmiş verilerin mevcudiyeti, tespit edilecek anormalliklerin türü ve benzeri gibi çeşitli faktörler tarafından tetiklenir. Genellikle bu faktörler, anormalliklerin tespit edilmesi gereken uygulama alanı tarafından belirlenir. Araştırmacılar, istatistik, makine öğrenimi, veri madenciliği, bilgi teorisi, spektral teori gibi farklı disiplinlerden kavramları benimsemiş ve bunları belirli problem formülasyonlarına uygulamışlardır [65].

3.3. Zaman Serileri

Teknolojideki son gelişmeler çeşitli araştırma alanlarında zaman içinde büyük miktarda veri toplamamızı sağlar. Sıralı bir şekilde kaydedilen ve zamanla ilişkilendirilen gözlemler bir zaman serisini oluşturur. Zaman serisi veri madenciliği, bu verilerden tüm anlamlı bilgileri çıkarmayı amaçlar ve sınıflandırma, kümeleme, tahmin, anomali tespiti çeşitli madencilik görevleri için ele alınmıştır [66-68].

3.4. Zaman Serilerinde Anomali Algılama Taksonomisi

Zaman serisi verilerinde aykırı değer saptama teknikleri, girdi veri tipine, aykırı değer tipine ve yöntemin doğasına bağlı olarak değişir. Bu nedenle bu üç yönü kapsayan kapsamlı bir taksonomi önerilmektedir. Şekil 3.3'te taksonomi sunulmuştur [8].



Şekil 3.3. Zaman serilerinde anomali tespit teknikleri.

3.4.1. Giriş verileri

Giriş değişkenlerinin türünü temsil eder. Tek değişkenli veya çok değişkenli zaman serileridir.

Tek değişkenli bir zaman serisi $X = \{x_t\}_{t\in T}$ her gözlemin belirli bir zamanda $t \in T \subseteq \mathbb{Z}^+$ kaydedildiği gerçek değerli gözlemlerin sıralı bir kümesidir. x_t, t anında toplanan değer veya gözlemdir ve $p, t \in T$ ve $p \leq |T| - n + 1$ için X zaman serisinde p konumundan başlayarak $S = x_p, x_{p+1}, \dots, x_{p+n-1}$, $n \leq |T|$ uzunluğundaki alt dizisidir. Her x_t gözlemi belirli bir X_t değişkeninin gerçekleşen değeridir [8].

Çok değişkenli zaman serisi $\boldsymbol{X} = \{\boldsymbol{x}_t\}_{t\in T}$ belirli bir zamanda $t \in T \subseteq \mathbb{Z}^+$ kaydedilen $k-$ boyutlu vektör kümesidir ve k gerçek değerli gözlemlerdir $\boldsymbol{x}_t = (x_{1t}, \dots, x_{kt})$. $\boldsymbol{x}_t$, bir değer veya gözlemdir ve $p, t \in T$ ve $p \leq |T| - n + 1$ için X çok değişkenli zaman serisinde $S = x_p, x_{p+1}, \dots, x_{p+n-1}$, $n \leq |T|$ uzunluğundaki alt dizisidir. Her $j \in \{1, \dots, k\}$, $X_j = \{x_{jt}\}_{t\in T}$ boyutu için tek değişkenli bir zaman serisidir ve $\boldsymbol{x}_t$ vektöründeki her x_{jt} gözlemi, $\boldsymbol{X}_T = (X_{1t}, \dots, X_{kt})$'deki rastgele zamana bağlı bir değişkenin gerçekleşen X_{jt} değeridir. Çok değişkenli zaman serilerinde her değişken yalnızca geçmiş değerlerine değil diğer zamana bağlı değişkenlere de bağlı olabilir [8].

3.4.2. Anomali türleri

3.4.2.1. Nokta anomaliler

En basit anomali türüdür ve anomali tespiti üzerine yapılan araştırmaların çoğunun odak noktasıdır. Normal bölgelerin sınırlarının dışında yer alırlar ve bu nedenle normal veri noktalarından farklı oldukları için nokta anomalileridir. Örneğin bir bireyin kredi kartı işlemlerinden tek bir özellik olarak harcanan miktarı baz alalım. Harcanan tutar o kişinin normal harcama aralığına göre çok yüksek olduğu bir işlem nokta anomalisi olarak adlandırılır [8].

3.4.2.2. Bağlamsal anomaliler

Verilerin bazı durumlarda normal bazı durumlarda anormal olarak değerlendirilebilir. Bu anomali davranış özel bir bağlamda gösteriliyorsa bu durum bağlamsal anomali (koşullu anomali) olarak adlandırılır. Bu özellik, bağlamsal bir anormallik saptama tekniği için bağlamsal ve davranışsal özniteliklerin belirlenmesinde anahtardır [8].

Örneğin bir bireyin kredi kartındaki satın alma zamanı bağlamsal bir özellik olabilir. Bireyin sevgililer gününde harcamasının 1000TL'ye ulaştığı gün dışında genellikle günlük 50TL'lik bir harcaması olduğunu düşünelim. Sevgililer gününde aynı miktarda harcanan miktar normal kabul edilecek olsa da diğer zamanda 1000TL'lik harcama, zaman bağlamında bireyin normal davranışına uymadığı için bağlamsal bir anormallik olarak kabul edilir [8].

3.4.2.3. Toplu anomaliler

Birbirleriyle ilişkili olan veriler, veri seti içerisinde anomali davranış oluşturuyorsa toplu anomali olarak adlandırılır. Toplu anomalide veri örnekleri tek başlarına anomali olmayabilir ancak bir arada toplu olarak bulunmaları anomalidir [8].

Örneğin aşağıda gösterildiği gibi bir bilgisayarda meydana gelen bir dizi eylemi ele alalım:

... http-web, buffer-overflow, http-web, http-web, smtp-mail, ftp, http-web, ssh, smtp-mail, http-web, ssh, buffer-overflow, ftp, http-web, ftp, smtp-mail, http-web ...

Bu örnek olay dizisi uzak bir makine tarafından yapılan tipik bir Web tabanlı saldırıya ve ardından ana bilgisayardan ftp yoluyla uzak bir hedefe veri kopyalamaya karşılık

gelir. Bu olay toplu anomali olduğu gibi olay dizisindeki durumlar tek başlarına değerlendirildiklerinde anormallik olmadığı unutulmamalıdır.

Nokta anormallikleri herhangi bir veri setinde meydana gelebilirken, toplu anormalliklerin yalnızca veri örneklerinin ilişkili olduğu veri setlerinde meydana gelebileceğine dikkat edilmelidir. Aksine, bağlamsal anormalliklerin oluşumu, verilerdeki bağlam özniteliklerinin mevcudiyetine bağlıdır. Bir nokta anomalisi veya toplu bir anomali, bir bağlama göre analiz edilirse, bağlamsal bir anomali olabilir. Bu nedenle, bir nokta anormallik tespit problemi veya toplu anormallik tespit problemi, bağlam bilgisi dahil edilerek bağlamsal bir anormallik tespit problemine dönüştürülebilir [65].

3.4.3. Yöntemin doğası

Kullanılan algılama yönteminin doğasını analiz eder (yani, algılama yönteminin tek değişkenli mi yoksa çok değişkenli mi olduğu). Tek değişkenli bir tespit yöntemi yalnızca tek bir zamana bağlı değişkeni dikkate alırken, çok değişkenli bir tespit yöntemi aynı anda birden fazla zamana bağlı değişkenle çalışabilir. Girdi verileri çok değişkenli bir zaman serisi olsa bile tespit yönteminin tek değişkenli olabileceğini unutmayın, çünkü değişkenler arasında var olabilecek bağımlılıklar dikkate alınmadan zamana bağlı her değişken üzerinde ayrı bir analiz yapılabilir. Buna karşılık, girdi verileri tek değişkenli bir zaman serisiyse, çok değişkenli bir teknik kullanılamaz [65].

3.5. K-Ortalamalar

Kümeleme, ham verileri mantıklı bir şekilde sınıflandıran ve veri kümelerinde var olabilecek gizli kalıpları araştıran bir yoldur [69]. Aynı kümedeki veriler benzer, ancak farklı kümeye ait veriler farklılık gösterecek şekilde veri nesnelerini ayrık kümeler halinde gruplandırma işlemidir [70].

K-means, sayısal, denetimsiz, deterministik olmayan, yinelemeli bir yöntemdir. Basit ve çok hızlıdır, bu nedenle birçok pratik uygulamada, yöntemin iyi kümeleme sonuçları üretebilen çok etkili bir yol olduğu kanıtlanmıştır. Ancak küresel kümeler oluşturmak için çok uygundur. Araştırmacılar tarafından k-means algoritmalarının etkinliğini artırmak için birkaç girişimde bulunulmuştur [71].

Ağırlıklara dayalı geliştirilmiş bir k-means algoritması vardır. Bu sayısal öznitelik verilerini işleyebilen yeni bir bölümleme kümeleme algoritmasıdır ve ayrıca sembol öznitelik verilerini de işleyebilir. Bu yöntem izole noktaların etkisini ve "gürültüyü" azaltır, böylece kümelemenin verimliliğini artırır. Ancak bu yöntemin zamanın karmaşıklığı konusunda bir iyileştirmesi yoktur [70].

İlk küme merkezlerini bulmak için sistematik bir yöntem önerilmiştir. Bu yöntemle elde edilen bu merkezler, verilerin dağılımı ile tutarlıdır. Dolayısıyla bu yöntem, standart k-ortalamalar algoritmasından daha doğru kümeleme sonuçları üretebilir, ancak bu yöntemin dezavantajı ise yürütme süresi ve algoritmanın zaman karmaşıklığıdır [72].

K-means algoritması süreci: K-means, veri madenciliğinde kullanılan tipik bir kümeleme algoritmasıdır. Büyük veri setlerini kümelemek için yaygın olarak kullanılır. Küme problemlerini çözmek için uygulanan en basit denetimsiz öğrenme algoritmalarından biridir [73].

Verilen nesneler yineleme yoluyla minimum k farklı kümeye sınıflandırılır. Oluşturulan kümelerin sonuçları kompakt ve bağımsızdır [74].

Algoritma iki ayrı aşamadan oluşmaktadır. İlk aşama, k değerinin önceden sabitlenen k merkezi rastgele seçilir. Bir sonraki aşama, her bir veri nesnesini en yakın merkeze götürür. Öklid mesafesi genellikle her bir veri nesnesi ile küme merkezleri arasındaki mesafeyi belirlemek için kabul edilir. Tüm veri nesneleri bazı kümelere dahil edildiğinde ilk adım tamamlanmış olur ve erken bir gruplandırma yapılır. Erken oluşan kümelerin ortalamasının yeniden hesaplanması yapılır. Bu yinelemeli süreç, kriter fonksiyonu minimum olana kadar tekrar tekrar devam eder [71].

Hedef nesnenin x olduğunu varsayarsak x_i, C_i kümesinin ortalamasını gösterir, kriter fonksiyonu aşağıdaki gibi tanımlanır:

$$E = \sum_{i=1}^{k} \sum_{x \in C_i} |x - x_i|^2 \tag{3.3}$$

E, veritabanındaki tüm nesnelerin kare hatasının toplamıdır. Kriter fonksiyonunun mesafesi, her bir veri nesnesi ile küme merkezi arasındaki en yakın mesafeyi belirlemek için kullanılan Öklid mesafesidir. Bir x=(x1 ,x2 ,…xn) vektörü ile başka

bir y=(y1 ,y2 ,…yn) vektörü arasındaki Öklid mesafesi d(xi, yi) aşağıdaki gibi elde edilebilir:

$$d(x_i, y_i) = \left| \sum_{i=1}^{n} (x_i - y_i)^2 \right|^{\frac{1}{2}} \quad (3.4)$$

K-means algoritmasının adımları:

Giriş: İstenen küme sayısı - k ve n veri nesnesi içeren bir veritabanı D={d_1, d_2,…d_n}

Çıkış: K küme sayısı

Adımlar

1) İlk küme merkezi olarak D veri kümesinden k veri nesnesini rastgele seçilir.
2) Tekrarlanır;
3) Verisetinde her nesne d_i (1 <=i<=n) ile tüm k küme merkezleri c_j(1<=j<=k) arasındaki mesafe hesaplanır ve d_i veri nesnesi en yakın kümeye atanır.
4) Her j kümesi için (1<=j<=k), küme merkezini yeniden hesaplanır.
5) Kümelerin merkezinde değişiklik olmayana kadar tekrarlanır.

Algoritma her yinelemede her veri nesnesinden her küme merkezine olan mesafeyi hesaplamak zorundadır ve küme sayısının baştan belirlenmesinin gerekmesi dezavantaj olarak görülmektedir. Ayrıca küme merkezleri her seferinde rastgele seçildiğinden algoritma her çalışmada farklı sonuçlar üretebilmektedir [75].

3.6. Ağaç Temelli Modeller

3.6.1. Karar ağaçları

Tümevarımsal çıkarım, somut örneklerden genel modellere geçme sürecidir. Karar ağaçlarının amacı, sınıfları bilinen bir dizi örneği analiz ederek nesnelerin nasıl sınıflandırılacağını öğrenmektir. Örnekler tipik olarak nitelik-değer vektörleri olarak temsil edilir. Öğrenme girdisi, her biri bilinen bir sınıfa ait olan bu tür vektörlerden oluşur ve çıktı, nitelik değerlerinden sınıflara bir eşlemeden oluşur. Bu eşleme hem verilen örnekleri hem de diğer görünmeyen örnekleri doğru bir şekilde sınıflandırmalıdır [76].

Karar ağacı eşlemeleri ifade etmek için kullanılan yöntemdir. İki veya daha fazla alt ağaç ve yaprağa bağlı testlerden veya nitelik düğümlerinden veya karar anlamına gelen

bir sınıfla etiketlenmiş karar düğümlerinden oluşur. Bir test düğümü, bir örneğin öznitelik değerlerine dayalı olarak bazı sonuçları hesaplar ve her olası sonuç alt ağaçlardan biriyle ilişkilendirir. Bir örnek, ağacın kök düğümünden başlayarak sınıflandırılır. Bu düğüm bir test ise, örneğin sonucu belirlenir ve uygun alt ağaç kullanılarak işlem devam eder. Örneğin tahmin edilen sınıfı karşılaşılan yaprağın etiketidir.

Karar ağaçlarının yardımıyla bir çözüm bulmak için bir dizi çözülmüş veriseti hazırlamak gerekir. Tüm veriseti daha sonra bir karar ağacının başlatılması için kullanılan bir eğitim seti ve elde edilen bir çözümün doğruluğunu kontrol etmek için kullanılan bir test seti olarak ikiye ayrılır. İlk olarak, her durumu tanımlayan tüm öznitelikler tanımlanır (girdi verileri) ve aralarından verilen problem için bir kararı temsil eden bir öznitelik seçilir (çıktı verileri). Tüm giriş nitelikleri için belirli değer sınıfları tanımlanır. Bir öznitelik birkaç ayrı değerden yalnızca birini alabiliyorsa, o zaman her değer kendi sınıfını alır; Bir öznitelik çeşitli sayısal değerler alabiliyorsa, farklı sınıfları temsil eden bazı karakteristik aralıkların tanımlanması gerekir. Her öznitelik, öznitelik düğümü veya test düğümü olarak da adlandırılan, oluşturulmuş bir karar ağacında bir dahili düğümü temsil edebilir. Bir karar ağacının yaprakları kararlardır. Çözülmemiş bir vaka için bir karar verilmesi gerektiğinde, karar ağacının kök düğümü ile başlarız ve öznitelik düğümleri boyunca ilerleyerek çözülmemiş durumdaki uygun özniteliklerin değerlerinin karar ağacındaki öznitelik değerleriyle eşleştiği dallar seçilir ve kararı temsil eden düğüme ulaşılır [77].

3.6.2. Torbalama

Karar ağaçlarının varyansı yüksek olduğundan dolayı verideki küçük bir değişim büyük bir etkiye sahiptir. Bu yüzden dolayı modelin yorumlanması zorlaşmaktadır. Bu yüzden torbalama kullanılır. Boostrap örneklemesi kullanılır. Bireysel modellerin ortalaması alınarak toplulaştırılır. Ensemle model oluşturmanın en basit yöntemi ortalama almadır. Torbalama yöntemi aşırı uyumu engeller [62].

Bootsrap sampling (Bootstrapping): Eğitim veri setinden örnekler yinelemeli olarak rastgele seçilir. Bu durumda eğitim veri setinden bazı örnekler birden fazla seçilebileceği gibi bazı örnekler hiç seçilmeyebilir. Bu sonuçlar eğitim veri setinin modifiye edilmiş halidir. Bu model başlangıç verisine benzer veriler oluşturmaya yardımcı olur ve böylece çok sayıda benzer model oluşturulabilir [62].

3.6.3. Rastgele orman

Random Forest topluluk öğrenme yöntemidir. Veri setinden bootstrap tekniğini ile farklı örneklemler seçilerek karar ağaçları oluşturulur. Oluşan ağaçlar bir araya gelerek karar ormanını oluşturur. Orman nihai sınıf tahminini ağaçların yaptığı sınıf tahminlerini bir araya getirerek yapar.

Random Forest yöntemi bootsrap'ten farklı olarak ağaçları oluştururken tüm değişkenlerin yerine bu değişkenlerin alt kümelerini de dikkate alır. Böylelikle etkisi yüksek olan değişkenler her ağacı şekillendirmesi engellenmektedir.

3.6.4. Boosting

3.6.4.1. AdaBoost

1995 yılında Freund ve Schapire tarafından tanıtılan AdaBoost algoritması, daha önceki güçlendirme algoritmalarının birçok pratik zorluklarını çözmüştür [78].

AdaBoost Algoritması:

Verilen: $(x_i, y_i), \ldots, (x_m, y_m);\ x_i \in X, y_i \in Y = \{-1, +1\}$

Başlat $D_1(i) = 1/m$.

For t=1, … , T:

- D_t dağılımı kullanılarak modeli eğiti.
- Zayıf hipotezi elde et $h_t : X \rightarrow \{-1, +1\}$ hatasıyla birlikte

$$\epsilon_t = Pr_{i \sim D_t}[h_t(x_i) \neq y_i].$$

- Seç $\alpha_t = \frac{1}{2}\ln\left(\frac{1-\epsilon_t}{\epsilon_t}\right)$.
- Güncelle:

$$D_{t+1}(i) = \frac{D_t(i)}{Z_t} \times \begin{cases} e^{-\alpha t} & \text{if } h_t(x_i) = y_i \\ e^{\alpha t} & \text{if } h_t(x_i) \neq y_i \end{cases}$$

$$= \frac{D_t(i)\exp\left(-\alpha_t y_i h_t(x_i)\right)}{Z_t}$$

burada Z_t bir normalleştirme fonksiyonudur.

Çıkış/Son Hipotez:

$$H(x) = \text{sign}\left(\sum_{t=1}^{T} \alpha_t h_t(x)\right) \tag{3.5}$$

Algoritma girdi olarak bir eğitim seti alır (x_1; y_1), … , (x_m; y_m). Burada her xi, X'in etki alanına veya örnek uzayına aittir ve her y_i etiketi Y etiket kümesi içinde yer alır. $Y = \{-1, +1\}$; olduğunu varsaysak çok sınıflı durumun uzantılarını incelemek gerekir. AdaBoost bir dizi tur içerisinde temel öğrenme algoritmasını tekrar tekrar kullanır. Algoritmanın ana amaçlarından biri, eğitim süresi boyunca ağırlık dağılımını veya kümesini korumaktır. t turundaki i eğitim örneğinin ağırlığı $D_t(i)$ ile gösterilir. Başlangıçta tüm ağırlıklar eşit olarak ayarlanır fakat her turda yanlış sınıflandırılan örneklerin ağırlıkları artırılır. Böylece eğitim setindeki zor örneklere odaklanmak zorunda kalır. Zayıf hipotezlerin performansı hata değerleri ile ölçülür.

$$\epsilon_t = \Pr_{i \sim D_t}[h_t(x_i)] \neq y_i = \sum_{i:h_t(x_i) \neq y_i} D_t(i) \tag{3.6}$$

Hata zayıf öğrenenin eğitildiği D_t dağılımına göre ölçülür. Bunun mümkün olmadığı durumlarda eğitim örnekleri D_t'nin alt kümesine göre örneklendirilebilir. Bu yeniden örneklenen durumlar zayıf öğreneni eğitmek için kullanılabilir [79].

3.6.4.2. Gradyan yükseltme makineleri

Gradyan Yükseltme Makinelerinde (GBM) öğrenme prosedürü yanıt değişkeninin daha doğru tahminini sağlamak için art arda yeni modeller denemektir. Algoritmanın arkasındaki temel fikir ise yeni temel öğrenicileri, tüm toplulukla ilişkili kayıp fonksiyonunun negatif gradyanı ile maksimum düzeyde ilişkilendirilecek şekilde oluşturmaktır [80].

Gradyan yükseltme çok çeşitli uygulamalarda önemli başarılar göstermiş makine öğrenimi teknikleri arasında yer alır. Uygulamanın amacına göre yöntem son derece özelleştirilebilir [81].

Model tasarımına çok fazla özgürlük sağlanmasından dolayı en uygun kayıp fonksiyonunun seçimi bir deneme yanılma yöntemi ile belirlenebilir. Boosting algoritmalarının uygulaması basittir bu sayede kişilere farklı model tasarımlarıyla deney yapma olanağı tanır.

Gradyan Yükseltme Algoritması: İsteğe bağlı olarak hem kayıp fonksiyonu hem de temel öğrenen modelleri belirtilebilir. Uygulamada, belirli bir kayıp fonksiyonu $\Psi(y, f)$ ve/veya özel bir temel öğrenici $h(x, \theta)$ verildiğinde, parametre tahminlerinin çözümünü elde etmek zor olabilir. Bunu engellemek için, gözlemlenen veriler boyunca

negatif gradyana $\{g_t(x_i)\}_{i=1}^{N}$ en paralel olacak yeni bir $h(x, \theta_t)$ fonksiyonunun seçilmesi önerilir:

$$g_t(x) = E_y \left[\frac{\partial \Psi\big(y, f(x)\big)}{\partial f(x)} | x \right]_{f(x)=f^{t-1}(x)} \tag{3.7}$$

Boost artışı için genel çözümü fonksiyon uzayında aramak yerine $-g_t(x)$ ile en fazla ilişkili fonksiyon seçilebilir. Bu potansiyel olarak çok zor bir optimizasyon görevinin en küçük kareler minimizasyonu ile değiştirilmesine izin verir [81]:

$$(\rho_t, \theta_t) = \arg \min_{\rho,\theta} \sum_{i=1}^{N} [-g_t(x_i) + \rho h(x_i, \theta)]^2 \tag{3.8}$$

Belirli bir görev için belirli bir GBM tasarlamak için, $\Psi(y, f)$ ve $h(x, \theta)$ fonksiyonel parametrelerine seçenekler sağlanmalıdır. Gerçekte neyin optimize edileceğini belirtmeli ve ardından çözümü oluştururken kullanılacak fonksiyonun biçimini seçmelidir. Bu seçimler GBM model özellikleri büyük ölçüde etkiler.

GBM'lerin dezavantajı ise aşırı uyum problemi(overfitting) eğilimlidirler. Bu yüzden dolayı eğitim verisinin bir kısmı ayrı tutulmalı ve/veya 'early stopping' kullanılmalıdır [62].

XGBoost: Bir ölçeğe göre ölçülebilir veya derecelendirilebilir makine öğrenme modelidir. Ağaç yapılarını güçlendirmek için kullanılır. Modelin performansı zorlu makine öğrenmesi ve veri madenciliği süreçlerinde test edilmiş ve geniş çapta kabul görmüştür. Etki alanına bağlı veri analizi ve özellik mühendisliği bu çözümlerde önemli bir rol oynamakla birlikte, XGBoost'un öğrenenlerin fikir birliği dayanan tercihi olması, sistemimizin ve ağaç güçlendirmemizin etkisini ve önemini göstermektedir [82].

XGBoost'un başarısının arkasındaki en önemli faktör, tüm senaryolarda ölçeklenebilir olmasıdır. Mevcut popüler çözümlerin toplandığı bir makinadan on kat daha hızlı çalışır ve dağıtılmış veya sınırlı bellek ayarlamalarında milyarlarca örneği ölçeklendirebilir. Birkaç önemli sistem ve algoritmik optimizasyondan sayesinde XGBoost ölçeklenebilir. Bu yenilikler; seyrek verileri işlemek için yeni bir ağaç öğrenme algoritması, yaklaşık ağaç öğrenmede teorik olarak doğrulanmış bir ağırlıklı nicel çizim prosedürünü örnek ağırlıklarının işlenmesine sağlamasıdır. Daha da önemlisi, XGBoost çekirdek dışı hesaplamadan yararlanır ve veri bilimcilerin bir

masaüstünde yüz milyonlarca örneği işlemesine olanak tanır ve en az miktarda küme kaynağıyla daha da büyük verilere ölçeklenen uçtan uca bir sistem oluşturmak için bu teknikleri birleştirir.

$$\mathcal{L}_{split} = \frac{1}{2}\left[\frac{\left(\sum_{i\in I_L} g_i\right)^2}{\sum_{i\in I_L} h_i + \lambda} + \frac{\left(\sum_{i\in I_R} g_i\right)^2}{\sum_{i\in I_R} h_i + \lambda} - \frac{(\sum_{i\in I} g_i)^2}{\sum_{i\in I} h_i + \lambda}\right] - \gamma \qquad (3.9)$$

Ağaç öğrenmedeki kilit sorunlardan biri denklem 3.9'da gösterildiği gibi en iyi ayrımı bulmaktır. Bunu yapabilmek için bütün özelliklerin olası bütün bölünmeleri numaralandırılır. Bu açgözlü algoritma olarak adlandırılır. XGBoost'un tek makine versiyonu gibi mevcut çoğu tek makineli ağaç yükseltme uygulamaları tam açgözlü algoritmayı destekler. Sürekli özellikler için tüm olası bölmeleri numaralandırmak hesaplama açısından zordur. Bunu verimli bir şekilde yapmak için, algoritmanın önce verileri özellik değerlerine göre sıralaması ve denklem 3.9'da ki yapı puanı için gradyan istatistiklerini toplamak üzere verileri sıralı sırayla kontrol etmesi gerekir [83,84].

Ağırlıklı parçalı sketch (Weighted Quantile Sketch): Aday ayırma noktalarının önerilmesi tahmin algoritmalarında çok önemli bir yere sahiptir. Adayların veriler üzerinde eşit olarak dağılmasını sağlamak için genellikle bir özelliğin yüzdelik dilimleri kullanılır. Biçimsel olarak, çoklu dizi $D_k = \{(x_{1k}, h_1), (x_{2k}, h_2), \dots, (x_{nk}, h_n)\}$ k'inci özellik değerlerini ve her eğitim örneğinin ikinci dereceden gradyan istatistikleri temsil eder. Bir derecelendirme fonksiyonu rk tanımlanabilir: $r_k : \mathbb{R} \to [0, +\infty)$ gibi

$$r_k(z) = \frac{1}{\sum_{(x,h)\in D_k} h} \sum_{(x,h)\in D_k, x<z} h \qquad (3.10)$$

özellik değeri z'den küçük olan k örneklerin oranını temsil eder. Amaç aday ayrım noktalarını $\{s_{k1}, s_{k2}, \dots, s_{kl}\}$ bulmaktır, öyle ki

$$\left|r_k(s_{k,j}) - r_k(s_{k,j+1})\right| < \epsilon\,, s_{k1} = \min_i x_{ik}\,, s_{k1} = \max_i x_{ik}. \qquad (3.11)$$

Burada ϵ bir yaklaşım faktörüdür. Sezgisel olarak bu, kabaca $1/\epsilon$ aday puan olduğu anlamına gelir. Burada her veri noktası h_i ile ağırlıklandırılır. h_i 'nin neden ağırlığı temsil ettiğini görmek için denklem aşağıdaki gibi yazabilir:

$$\sum_{i=1}^{n} \frac{1}{2} h_i (f_t(x_i) - g_i/h_i)^2 + \Omega(f_t) + constant \quad (3.12)$$

g_i/h_i etiketleri ve h_i ağırlıkları ile tam olarak ağırlıklı kare kaybıdır. Büyük veri kümeleri için, kriterleri karşılayan aday bölmeleri bulmak önemlidir. Her örnek eşit ağırlığa sahip olduğunda, nicelik çizimi (quantile sketch) adı verilen mevcut bir algoritma sorunu çözer [85,86].

Daha sonradan ise ağırlıklı veri kümeleri için ise ağırlıklandırılmış quantile sketch adında yeni bir algoritma geliştirilmiştir.

Seyreklik uyumu (Sparsity-aware Split Finding): Birçok problemde giriş değişkenlerinin seyrek olması durumuyla karşılaşılabilir. Seyrekliğin birden çok olası nedeni vardır:

- Verilerde eksik değerlerin varlığı
- İstatistiklerde sık sık sıfır girişleri
- One-hot encoding gibi öznitelik mühendisliği sonuçları

Tasarlanan algoritmanın veri üzerindeki seyreklik örüntülerinin farkında olması önemlidir. Bu yüzden tasarımda, her ağaç düğümüne varsayılan bir yön eklemek önerilmektedir. 'Seyrek x matrisinde bir değer eksik olduğunda, örnek varsayılan yönde sınıflandırılır.' Her dalda iki varsayılan yön seçeneği bulunmaktadır. Uygun olan varsayılan yönler verilerden öğrenilmektedir.

XGBoost algoritma adımları:

Giriş: I, geçerli düğümün örnek kümesi

Giriş: $I_k = \{i \in I \mid x_{ik} \neq \text{missing}\}$

Giriş: d, özellik boyutu

$G \leftarrow \sum_{i \in I} g_i, H \leftarrow \sum_{i \in I} h_i$

for $k = 1$ to m do

$G_L \leftarrow 0,\ H_L \leftarrow 0$

for $j\ in\ sorted$ do

$G_L \leftarrow G_L + g_j, H_L \leftarrow H_L + h_j$

$G_R \leftarrow G - G_L, H_R \leftarrow H + H_L$

$score \leftarrow \max\left(score, \frac{G_L^2}{H_L + \lambda} + \frac{G_R^2}{H_R + \lambda} - \frac{G^2}{H + \lambda}\right)$

end

$G_R \leftarrow 0,\ H_R \leftarrow 0$

for $j\ in\ sorted$ do

$G_R \leftarrow G_R + g_j, H_R \leftarrow H_R + h_j$

$G_L \leftarrow G - G_R, H_L \leftarrow H + H_R$

$score \leftarrow \max\left(score, \frac{G_L^2}{H_L + \lambda} + \frac{G_R^2}{H_R + \lambda} - \frac{G^2}{H+\lambda}\right)$

end

end

Çıkış: Maksimum kazançlı bölünmüş ve varsayılan yönler

Algoritmadaki temel iyileştirme yalnızca eksik olmayan girişleri (I_k) hesaplamaya katılmasıdır. Sunulan algoritma, var olmama durumunu eksik bir değer olarak değerlendirir ve eksik verileri işlemek için en iyi yönü öğrenir. Bu algoritma sayesinde var olmayan veriler eksik veri olarak değerlendirilip çözüme ulaşabildiği gibi kullanıcının kriterlerine göre de çözüm sürecinde değerlendirilmeye katılmaması gereken girişleri belirleyip algoritmanın en iyi yönü öğrenmesi gerçekleşmektedir.

Mevcut ağaç öğrenme algoritmalarının çoğu ya yalnızca yoğun veriler için optimize edilmiştir ya da kategorik kodlama gibi sınırlı durumların üstesinden gelmek için özel prosedürlere ihtiyaç duyar. XGBoost, tüm seyreklik modellerini birleşik bir şekilde işler. Bu yöntem, hesaplama karmaşıklığını giriş değişkenlerinde eksik olmayan girişlerin sayısını doğrusal hale getirmek için seyrekliği kullanır [87]. XGBoost parametrelerine EK A1'de yer verilmiştir.

LightGBM: Büyük verilerin ortaya çıkmasıyla birlikte (hem özellik sayısı hem de örnek sayısı açısından), GBDT özellikle doğruluk ve verimlilik arasındaki dengede yeni zorluklarla karşılaşmıştır [81].

GBDT'nin geleneksel uygulamalarının, olası tüm ayrılma noktalarının kazancını tahmin etmek için her özellik için tüm veri örneklerini taraması gerekir. Bu nedenle hem özellik sayısı hem de örnek sayısı ile doğru orantılı olarak hesaplama karmaşıklıkları ortaya çıkmaktadır. Bu, büyük verileri işlerken bu uygulamaları çok zaman alıcı hale getirir.

Bu zorluğun üstesinden gelmek için veri örneklerinin sayısını ve özellik sayısını azaltmak düşünülebilir. Ancak, yapılan çalışmalar bunun önemsiz olduğu ortaya

çıkarıyor. Çünkü GBDT için veri örneklemenin nasıl gerçekleştirileceği belli değildir. Boost eğitim sürecini hızlandırmak için verileri ağırlıklarına göre örnekleyen çalışmalar vardır. Fakat GBDT'de hiç örnek ağırlık olmadığı için doğrudan GBDT'ye uygulanamazlar.

Bu yüzden Gradient-based One- Side Sampling (GOSS) ve Exclusive Feature Bundling (EFB) teknikleriyle gradyan yükseltme algoritması geliştirilerek bu gibi zorlukların üstesinden gelebilen LightGBM algoritması önerilmiştir.

GOSS: Veri setinden örneklem oluşturulurken doğruluk değerini etkilemeden bilgi kazancını hesaplarken önemli verileri kullanarak veri sayısının azaltılması sağlar.

EFB: Seyrek özellikler birleştirilerek yoğun özellik paketleri oluşturulur ve bu pakette değişkenler birleştirilir. Bu sayede karmaşıklığın engellemesi ve hızlı eğitim sürecinin tamamlanması sağlanırken doğruluk oranına zarar vermeden değişken sayılarının azaltılması ve model eğitim performansının arttırılması amaçlar [88].

GBDT her bir ayrılma noktasını belirlemek için genellikle bilgi kazancını kullanılırken LightGBM varyans kazancını hesaplayarak GOSS'u kullanır [89].

Denetimli eğitim seti göz önüne alındığında $X = \{(x_i, y_i)\}_{i=1}^{n}$, LightGBM belirli bir işleve sahip $f^*(x)$ yaklaşım bulmayı amaçlar $\hat{f}(x)$, bu belirli bir kayıp fonksiyonunun $L\big(y, f(x)\big)$ beklenen değerini aşağıdaki gibi en aza indirir:

$$\hat{f} = \arg\min_{f} E_{y,X}, L\big(y, f(x)\big) \tag{3.13}$$

LightGBM, son modele yaklaşmak için bir dizi regresyon ağacını $\sum_{t=1}^{t} f_t\,(X)$ birleştirir,

$$f_T(X) = \sum_{t=1}^{T} f_t\,(X) \tag{3.14}$$

Regresyon ağaçları $w_{q(x)}, q \in \{1, 2, \dots, J\}$ şeklinde ifade edilebilir. Burada J yaprak sayısını, q ağacın karar kurallarını, w, yaprak düğümlerin örnek ağırlığını gösteren bir vektördür. Bu nedenle LightGBM t adımında ek bir formda eğitilmeli:

$$\Gamma_t = \sum_{i=1}^{n} L\big(y_i, F_{t-1}(x_i) + f_t(x_i)\big) \tag{3.15}$$

LightGBM'de amaç fonksiyonuna Newton'un yöntemiyle hızla yaklaşılır. Sabit terim sadeleştirmek için çıkardıktan sonra formülasyon aşağıdaki gibi dönüştürülebilir:

$$\Gamma_t \cong \sum_{i=1}^{n}\left(g_i, f_t(x_i) + \frac{1}{2}h_i, f_t^2(x_i)\right) \tag{3.16}$$

Burada g_i ve h_i kayıp fonksiyonunun birinci ve ikinci dereceden gradyan istatistiklerini gösterir. Yaprak j'nin örnek kümesini I_j temsil ettiğimizi düşünürsek formül aşağıdaki gibi dönüştürülebilir:

$$\Gamma_t = \sum_{j=1}^{j}\left(\left(\sum_{i\in I_j} g_j\right)w_j + \frac{1}{2}\left(\sum_{i\in I_j}(h_i+\lambda)\,w_j^2\right)\right) \tag{3.17}$$

Belirli bir ağaç yapısı q(x) için her bir yaprak düğümü w*j'nin optimum yaprak ağırlık puanları ve Γ_K'nin kesin değeri aşağıdaki gibi çözülebilir:

$$w_j^* = -\frac{\sum_{i\in I_j} g_i}{\sum_{i\in I_j} h_i + \lambda} \tag{3.18a}$$

$$\Gamma_T^* = -\frac{1}{2}\sum_{j=1}^{J}\frac{\left(\sum_{i\in I_j} g_i\right)^2}{\sum_{i\in I_j} h_i + \lambda} \tag{3.18b}$$

q ağaç yapısının kalitesini ölçen puanlama işlevi olarak Γ_T^* görülebilir. Son olarak, ayırmayı ekledikten sonraki amaç fonksiyonu şu şekildedir:

$$G = \frac{1}{2}\left(\frac{\left(\sum_{i\in I_L} g_i\right)^2}{\sum_{i\in I_L} h_i + \lambda} + \frac{(\sum_{i\in R} g_i)^2}{\sum_{i\in I_R} h_i + \lambda} - \frac{(\sum_{i\in I} g_i)^2}{\sum_{i\in I} h_i + \lambda}\right) \tag{3.19}$$

I_L ve I_R sırasıyla sol ve sağ dalların örnek kümeleridir. XGBoost ve GBDT gibi geleneksel GBDT tabanlı tekniklerin aksine, Light GBM ağacı dikey olarak büyütürken, diğer algoritmalar ağaçları yatay olarak büyütür, bu da LightGBM'yi büyük ölçekli veri ve özelliklerin işlenmesinde etkili bir yöntem haline getirmiştir.

Tahmin doğruluğu hiper parametrelerden önemli ölçüde etkilenir. Bu nedenle LightGBM'yi kullanmadan önce hiper parametresinin sayısını ve varyasyon aralığını belirlemek gerekir [90]. LightGBM parametrelerin EK A2'de yer verilmiştir.

CatBoost: CatBoost, temel tahmin ediciler gibi ikili karar ağaçlarını kullanan bir gradyan güçlendirme uygulamasıdır. Sınıflandırma yöntemleri içerisinde etkili bir makine öğrenmesi algoritmasıdır [91]. CAT önce tüm örnekleri rasgele sıralar ve ardından kategori tabanlı bir özellikten bir değer alır. Örnekten önce gelen kategori etiketine dayalı olarak ağırlık katsayılarını ekleyerek ortalama bir değerle her örnek özellik sayısal bir değere dönüştürülür. Yeni zayıf öğreniciler oluşturma sürecinde CAT modeli tahmin etmek için X_n örneğinden önce örnek noktaların gradyanını kullanır ve ardından bu modelleri X_n'nin gradyanını hesaplamak ve modeli güncellemek için kullanır [92].

Örnekleriyle bir veriyi $D = \{(X_j, y_j)\}_{j=1,\dots,m}$ incelediğimizi düşünürsek, burada $X_j = \{x_j^1, x_j^2, \dots, x_j^n\}$ n özellikte bir vektördür ve etkilenen özellik $y_i \in \mathbb{R}$ ikili olarak(evet veya hayır) veya sayısal özellik(0 veya 1) olarak ifade edilir. Örnekler (X_j, y_j) bağımsız ve bilinmeyen özelliklere $p(.,.)$ aynı şekilde sınıflandırılmış olabilir. Öğrenme görevinin amacı, aşağıda verilen formüldeki beklenen kaybı en aza indiren bir $H: \mathbb{R}^n \to \mathbb{R}$ fonksiyonunu eğitmektir.

$$\mathcal{L}(H) := \mathbb{E}L(y, H(X)) \tag{3.20}$$

Burada L(,) düzgün bir kayıp fonksiyonudur ve (X, y) eğitim verilerinden D örneklenen bir test verisidir.

Gradyan yükseltme yaklaşımı açgözlü bir şekilde yinelemeli olarak bir $H^t: \mathbb{R}^m \to \mathbb{R}, t = 0, 1, \dots$ yaklaşım dizisi oluşturur. Süreçte H^{t-1} önceki yaklaşımından H^t eklemeli olarak elde edilir. Adım boyutu α olan ve temel tahmin fonksiyonuna $g^t: \mathbb{R}^n \to \mathbb{R}$ sahip $H^t = H^{t+1} + \alpha g^t$ içinde tanımlanan beklenen kaybı azaltmak veya en aza indirmek için G fonksiyonundan seçilir [81].

$$g^t = \arg\min_{g \in G} \mathcal{L}(H^{t-1} + g) \tag{3.21a}$$

$$= \arg\min_{g \in G} \mathbb{E}\mathcal{L}(y, H^{t-1}(X) + g(X)) \tag{3.21b}$$

Minimizasyon problemlerine genellikle H^{t-1} 'de ikinci dereceden bir yaklaşım kullanan Newton yöntemi $\mathcal{L}(H^{t-1} + g^t)$ ile veya (negatif) bir gradyan adımı alınarak yaklaşılır [93].

3.7. Hata Ölçüm Parametreleri

Aşağıdaki formüllerde, i'inci değer için tahmini değer X_i ve Y_i ise gerçek değerdir. Regresyon yöntemi veri kümesinin karşılık gelen Y_i öğesi için X_i öğesini tahmin eder [94].

Gerçek değerlerin ortalaması:

$$\bar{Y} = \frac{1}{m}\sum_{i=1}^{m} Y_i \tag{3.22}$$

Ortalama toplam kareler toplamı:

$$\text{MST} = \frac{1}{m}\sum_{i=1}^{m} (Y_i - \bar{Y})^2 \tag{3.23}$$

3.7.1. Belirleme katsayısı

Belirleme katsayısı bağımsız değişkenler ile tahmin edilebilen bağımlı değişkenin varyans oranı olarak tanımlanır [94].

$$R^2 = 1 - \frac{\sum_{i=1}^{m}(X_i - Y_i)^2}{\sum_{i=1}^{m}(\bar{Y} - Y_i)^2} \tag{3.24}$$

3.7.2. Mean squared error (MSE)

Tespit edilmesi gereken aykırı değerlerde MSE kullanılabilir. MSE L_2 normu sayesinde bu tür değerlere daha büyük ağırlıklar verir. Model sonucu çıktılardan sadece bir kötü sonucun olması fonksiyonun kare kısmından dolayı hatayı büyütür. R^2 ve MST eldeki veriler için sabit olduğundan, R^2 monoton olarak MSE ile ilişkilidir. Bu R^2'ye dayalı regresyon modellerinin sıralamasının, MSE veya RMSE'ye dayalı modellerin sıralamasıyla aynı olacağı anlamına gelmektedir [95].

$$\text{MSE} = \frac{1}{m}\sum_{i=1}^{m} (X_i - Y_i)^2 \tag{3.25}$$

3.7.3. Root mean squared error (RMSE)

MSE'nin karekökü değeridir. MSE değerinin karşılaştırılamayacak kadar büyük olduğu durumlarda tercih edilir [95].

$$\text{RMSE} = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(X_i - Y_i)^2} \tag{3.26}$$

3.7.4. Mean absolute error (MAE)

MAE aykırı değerler verilerin bozuk kısımlarını temsil ettiği durumlarda kullanılır. Model için genel ve sınırlı bir performans ölçüsü sağlar. Test setinde çok sayıda aykırı değer varsa model performansı çok düşük çıkar [95].

$$\text{MAE} = \frac{1}{m}\sum_{i=1}^{m}|X_i - Y_i| \tag{3.27}$$

3.7.5. Mean absolute percentage error (MAPE)

MAPE göreli hata açısından çok sezgisel bir yorumu vardır. Mutlak değişikliklerden çok göreli değişikliklere duyarlı olmanın daha önemli olduğu görevlerde kullanılması tavsiye edilir [96].

Dezavantajı ise pozitif verilerle sınırlandırılması ve düşük tahminlere yönelik önyargılı olmasıdır, bu da büyük hataların beklendiği tahmin modelleri için uygun değildir [95,97].

$$\text{MAPE} = \frac{1}{m}\sum_{i=1}^{m}\left|\frac{Y_i - X_i}{Y_i}\right| \tag{3.28}$$

3.8. Karışıklık Matrisi

Bir karışıklık matrisi, bir sınıflandırma sistemi tarafından yapılan gerçek ve tahmin edilen sınıflandırmalar hakkında bilgi içerir. Bu tür sistemlerin performansı genellikle matristeki veriler kullanılarak değerlendirilir [98]. Tablo 3.1'de iki sınıf bir sınıflandırıcı için karışıklık matrisine yer vermiştir.

3.8.1. Doğruluk

Doğru olan tahminlerin toplam sayısının oranıdır [98].

$$\text{Doğruluk} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FN} + \text{FP} + \text{TN}} \tag{3.29}$$

Tablo 3.1. İki sınıf bir sınıflandırıcı için karışıklık matrisi.

		Tahmini Değerler	
		Pozitif	Negatif
Gerçek Değerler	Pozitif	Gerçek Pozitif (TP)	Yanlış Negatif (FN)
	Negatif	Yanlış Pozitif (FP)	Gerçek Negatif (TN)

3.8.2. Kesinlik

Doğru sınıflandırılan verilerin oranıdır [98].

$$\text{Kesinlik} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3.30}$$

3.8.3. Duyarlık

Sadece pozitif değerlerden doğru sınıflandırılanların oranıdır [98].

$$\text{Duyarlılık} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{3.31}$$

3.8.4. F ölçütü

Kesinlik ve duyarlılık değerlerinin harmonik ortalamasıdır [98].

$$\text{F-Ölçütü} = \frac{2\left(\frac{\text{TP}}{\text{TP} + \text{FP}}\right)\left(\frac{\text{TP}}{\text{TP} + \text{FN}}\right)}{\left(\frac{\text{TP}}{\text{TP} + \text{FP}}\right) + \left(\frac{\text{TP}}{\text{TP} + \text{FN}}\right)} \tag{3.32}$$

3.8.5. ROC ve AUC

Bir sınıflandırıcıdan daha doğru bir derece elde etmek istiyorsak eğitim örneklerinde gerçek sıralamaya ihtiyacımız olması beklenebilir [99]. Ancak çoğu senaryoda bu mümkün değildir. Veri kümemiz genelde yalnızca sınıf etiketlerine sahip örneklerden oluşur. Bu nedenle eğitim ve test setlerinde yalnızca sınıflandırma etiketleri verildiğinde, sınıflandırma derecelerini değerlendirirken ROC eğrisini doğruluktan daha iyi sonuçlar verir [100].

ROC eğrisi, ilk kez isabet oranları ile yanlış alarm oranları arasındaki dengeyi temsil etmek için sinyal algılama teorisinde kullanıldı [101,102]. 1970'lerden beri kapsamlı

bir şekilde çalışılmış ve tıbbi teşhiste uygulanmıştır [103,104]. Spackman, makine öğrenimi algoritmalarını karşılaştırmak ve değerlendirmek için ROC grafiğini kullanan ilk araştırmacılardan biridir [105]. Son yıllarda, makine öğreniminde ROC hakkında kapsamlı araştırmalar yapılmıştır [106,107].

ROC eğrisinin altındaki alan veya kısaca AUC, ROC eğrilerinin performansı için iyi bir özet sağlar. ROC eğrisi sınıflandırıcıların performansını tüm sınıf dağılımları ve hata maliyetleri aralığında karşılaştırır. Genellikle iki ROC eğrisi arasında yüksek ilişki yoktur. Bu durumlarda veya sınıf dağılımı ve hata maliyetleri bilinmediğinde ROC eğrisi altındaki alan veya kısaca AUC, iki ROC eğrisini karşılaştırmak için iyi bir durumdur [108].

AUC'yi ROC uzayında ROC eğrisi X'in altındaki alanı belirtmek için kullanılır. Bu nedenle, ROC eğrileri arasında baskınlık ilişkileri varsa, AUC değerleri ROC uzayındaki ROC eğrisi X altındaki bu hakimiyet ilişkilerini yansıtabilir. Bu önerinin tersi doğru değildir. Ancak AUC'nin özel bir istatistiksel anlamı vardır: rastgele seçilen bir negatif örneğin, pozitif sınıfa ait olma olasılığının, rastgele seçilen bir pozitif örneğe göre daha düşük olması olasılığını temsil eder [109].

Jin Huang yaptığı çalışmalarda AUC'nin öğrenme algoritmalarını karşılaştırmada doğruluğun yerini alması gerektiğini göstermiştir. Doğruluk kriterine göre öğrenme algoritmaları benzer sonuçlar gösterdiği halde AUC'a göre farklı oldukları ispatlanmıştır. Bu sonuçlara göre gerçek dünyadaki makine öğrenimi ve veri madenciliği uygulamalarında, öğrenme algoritmalarını optimizasyonunda ve karşılaştırmasında doğruluk yerine AUC'tan yararlanmamız gerektiğini gösteriyor [100].

4. UYGULAMA

4.1. HVAC Sistemine Ait Veri Seti

Gerçek bir HVAC sistemine erişimdeki sınırlamalar ve HVAC sistemlerinin siber güvenliğini araştırmak için halka açık etiketli veri setlerinin bulunmamasından dolayı enerji ve kütle dengesi denklemlerini kullanarak dinamik sistemlerin davranışını simüle etmeye olanak tanıyan bir yazılım olan TRNSYS kullanılarak bir simülasyon modelinden toplanan 12 bölgeli bir HVAC sisteminin veri seti kullanılmaktadır [110,111]. TRNSYS modelleri yetkili departmanlar tarafından pratik verilerle tutarlı olacak ve büyük ölçüde HVAC sistemini yeniden üretecek şekilde geliştirildiğinden HVAC sistemlerinin dinamiklerini simüle etmek için güvenilir bir araç olarak yaygın bir şekilde kullanılmaktadır [112].

Veri seti, soğutma uygulaması için simüle edilmiş 12 bölgeli bir HVAC sisteminden toplanmış. Tablo 4.1'de sunulduğu gibi, 1 dakikalık bir örnekleme hızında toplanan üç günlükten oluşmaktadır; burada Veri Kümesi 1, dört ay boyunca (Haziran'dan Eylül'e kadar) toplanan normal operasyonel verileri ve Veri Kümesi 2, 20 gün boyunca toplanan normal operasyonel verileri temsil eder. Veri kümesi 3, 20 günlük bir süre içinde enjekte edilen 16 saldırı verilerinden ve normal verilerden oluşur [111]. Veriseti ile ilgili detaylı bilgilendirmeye Ek A3 ve Ek A4'te yer verilmiştir.

Kullanılan saldırı modelleri aşağıdaki gibi 4 farklı grupta değerlendirilebilir [111].

Saldırı 1: Kontrol sisteminin ayar noktalarının değiştirilmesi

Saldırı 2: Değerlerini dondurarak veya bir önyargı oluşturarak sensör ölçümlerini tahrif etmek

Saldırı 3: Değerlerini dondurarak veya bir önyargı oluşturarak kontrol sinyallerini tahrif etmek

Saldırı 4: Komut sinyallerini bileşenlere değiştirme

Saldırıların detaylarına Tablo 4.2'de yer verilmiştir.

Tablo 4.1. Veri kümesi özellikleri.

Kayıt	Tip	Özellikler	Örnek sayısı
Veri kümesi 1	Normal	51 özellik: yılın saati, günün saati, sıcaklık sensörü ölçümleri, kontrol sinyalleri, ayar noktaları, sistem durumu.	194301
Veri kümesi 2	Normal	65 özellik: yılın saati, günün saati, sıcaklık sensörü ölçümleri, kontrol sinyalleri, ayar noktaları, bölgelerin termal konfor endeksleri, toplam tahmini güç kullanımı, sistem durumu.	194301
Veri kümesi 3	Normal ve saldırı	65 özellik: yılın saati, günün saati, sıcaklık sensörü ölçümleri, kontrol sinyalleri, ayar noktaları, bölgelerin termal konfor endeksleri, toplam tahmini güç kullanımı, sistem durumu.	8840

4.2. Scikit Learn

Python programlama dili bilimsel bilgi işlem için en popüler dillerden biridir. Yüksek düzeyde etkileşimli doğası ve olgunlaşan bilimsel kütüphaneler ekosistemi sayesinde, algoritmik geliştirme ve keşifsel veri analizi için çekici bir seçimdir [113,114]. Yalnızca akademik ortamlarda değil, aynı zamanda endüstride de giderek daha fazla kullanılmaktadır [115].

Scikit-learn, Python diliyle sıkı bir şekilde entegre edilmiş, kullanımı kolay bir arayüz sağlarken ve birçok iyi bilinen makine öğrenimi algoritmasının son teknoloji uygulamalarını sağlamak için bu zengin ortamı kullanır. Bu, yazılım ve web endüstrilerinde ve ayrıca biyoloji veya fizik gibi bilgisayar bilimi dışındaki alanlarda uzman olmayan kişiler tarafından istatistiksel veri analizine yönelik artan ihtiyaca cevap vermektedir [115]. Scikit-learn çeşitli nedenlerle Python'daki diğer makine öğrenimi kütüphanelerden farklıdır:

i) BSD lisansı altında dağıtılır
ii) MDP [116] ve pybrain'den [117] farklı olarak verimlilik için derlenmiş kod içerir

iii) R ve shogun gibi isteğe bağlı bağımlılıkları olan pymvpa'nın [118] aksine, kolay dağıtımı kolaylaştırmak için yalnızca numpy ve scipy'ye bağlıdır.

iv) Veri akışı çerçevesi kullanan pybrain'den farklı olarak zorunlu programlamaya odaklanır.

Tablo 4.2. Veri kümesi 3'te enjekte edilen saldırıların listesi.

Saldırı indeksi	Tanım	Saldırı zamanı
1.1	Chiller ayar noktasının 14 °C'ye değiştirilmesi	Gün 1, 12:00
1.2	Su deposunun ayar noktasının 16 °C'ye değiştirilmesi	Gün 2, 06:00
1.3	AHU ayar noktasının 20 °C olarak değiştirilmesi	Gün 2, 10:00
1.4	Bölge A1'in ayar noktasının 26 °C'ye değiştirilmesi	Gün 2, 11:00
1.5	Bölge C4'ün ayar noktasının 18 °C'ye değiştirilmesi	Gün 1, 03:00
2.1	Donma Bölgesi B1 okuması	Gün 5, 16:00
2.2	Donma Bölgesi C4 okuması	Gün 7, 06:00
2.3	Donma Bölgesi A2 okuması	Gün 9, 04:00
2.4	Donma Bölgesi C3 okuması	Gün 1, 06:00
2.5	Bölge B3'e 3 °C'lik bir sapma tanıtılması	Gün 3, 06:00
3.1	Bölge C2'nin kontrol sinyalinin dondurulması	Gün 1, 15:00
3.2	Bölge B3'ün kontrol sinyalinin dondurulması	Gün 13, 18:00
3.4	Bölge B1'in kontrol sinyalinin dondurulması	Gün 15, 06:00
3.5	Bölge B2'nin kontrol sinyalinin 0'a ayarlanması	Gün 19, 14:00
3.6	Bölge A3'ün kontrol sinyalini 1'e ayarlama	Gün 19, 20:00
4.1	AHU-B su pompasının hızının 1/3'üne düşürülmesi	Gün 18, 12:00

Paket çoğunlukla Python'da yazılmış olsa da, DVM'lerin referans uygulamalarını ve uyumlu lisanslarla genelleştirilmiş doğrusal modelleri sağlayan C++ kütüphanelerinden LibSVM [119] ve LibLinear'ı [120] içerir. Binary paketler, Windows ve herhangi bir POSIX platformu dahil olmak üzere zengin bir platform setinde mevcuttur [121].

Numpy: veri ve model parametreleri için kullanılan temel veri yapısıdır. Girdi verileri, numpy dizileri olarak tanımlanır, böylece diğer bilimsel Python kütüphaneleri ile sorunsuz bir şekilde işlem yapılabilir. Numpy'nin görüntüleme tabanlı bellek modeli,

derlenmiş kodla bağlarken bile kopyaları sınırlandırır [121]. Ayrıca temel aritmetik işlemler sağlar.

Scipy: lineer cebir, seyrek matris gösterimi, özel fonksiyonlar ve temel istatistiksel fonksiyonlar için verimli algoritmalar sağlar. Scipy, LAPACK gibi birçok Fortran tabanlı standart sayısal paket için birleşime sahiptir. Fortran kodu çerçevesinde kütüphaneler sağlamak çeşitli platformlarda zorlayıcı olabileceğinden, kurulum ve taşınabilirlik kolaylığı açısından bu önemlidir [115].

Scikit-learn, tutarlı, göreve yönelik bir arayüz kullanarak hem denetimli hem de denetimsiz çok çeşitli makine öğrenimi algoritmalarını ortaya çıkarır ve böylece belirli bir uygulama için yöntemlerin kolayca karşılaştırılmasını sağlar. Bilimsel Python ekosistemine dayandığından, geleneksel istatistiksel veri analizi aralığı dışındaki uygulamalara kolayca entegre edilebilir. Daha da önemlisi, yüksek seviyeli bir dilde uygulanan algoritmalar, bir kullanım durumuna özgü yaklaşımlar için yapı taşları olarak kullanılabilir [122].

4.3. Geliştirilen Uygulama

Python'da gerçekleştirilen uygulamanın adımları aşağıda sıralamıştır. Uygulamanın ayrıntılarına bir sonraki kısımda detaylı olarak yer verilecektir.

- Uygulamaya ait veri seti üzerinde bağımlı ve bağımsız değişken tanımları gerçekleştirilir.
- Kullanılacak algoritmalar proje üzerinde tanımlanır.
- Veri seti eğitim ve test amaçlıyla bölünerek algoritmalar eğitilir. Hata parametrelerine göre algoritma performansları karşılaştırılır.
- Eğitilen algoritmalar siber saldırıların bulunduğu veri seti üzerinde test edilir ve belirli bir eşik göre veriler anomali olarak etiketlenir.
- Algoritmaların anomali olarak etiketlediği veriler gerçek sonuçlar ile karşılaştırılarak karışıklık matrisi sonuçlarına göre değerlendirilir.
- En yüksek sonuç veren iki algoritma üzerinde model parametreleri üzerinde yapılan değişiklikler ile performans parametreleri kontrol edilir.
- Korelasyonel olarak veri seti giriş parametreleri üzerinde indirgeme işlemi yapılarak modeller tekrar oluşturulur ve performansları raporlanır.

- Gerçekleştirilen çalışma ile çok değişkenli zaman serileri üzerinde korelasyonel ilişki modeli uyguladıktan sonra model performansındaki değişim ispatlanacaktır.

4.4. Kullanılan Makine Öğrenmesi Yöntemleri Ve Parametreler

Bu bölümde LinearRegression (LR), DecisionTreeRegressor (DTR), KNeighborsRegressor (KNR), RandomForestRegressor (RFR) ve GradientBoostingRegressor (GBR) makine öğrenmesi algoritmalarına, performanslarına ve hata ölçüm parametrelerine yer verilmiştir. Farklı kategorilere ait makine öğrenmesi algoritmaları seçilerek daha kapsamlı karşılaştırma ve analiz yapabilme sağlanmıştır.

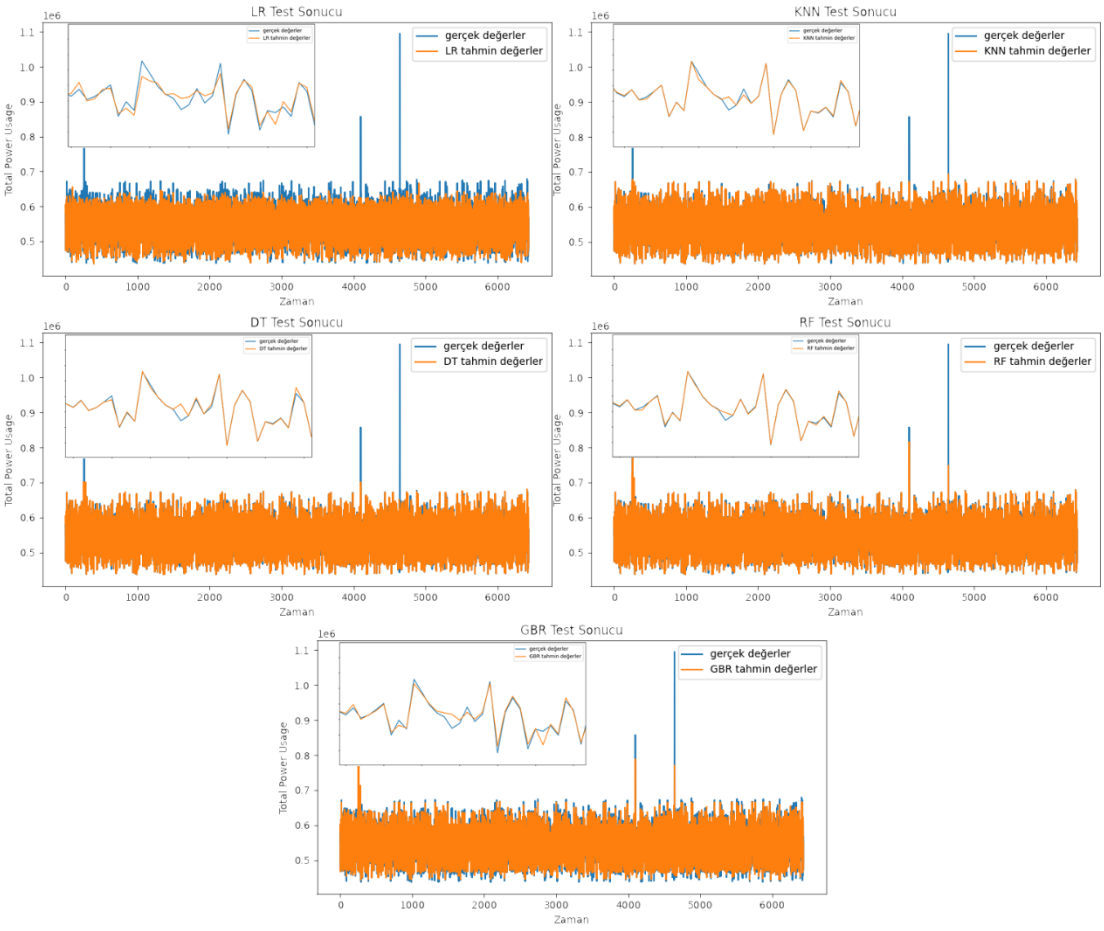
Veri kümesine 2'ye ait 194301 örneğin %80'i eğitim için %20'si test için ayrılmıştır. 49 parametre giriş olarak ve Total Power Using parametresi sistemin bağımlı değişkeni çıkış değeri olarak ayarlanmıştır.

Eğitim sonucunda algoritmaların test aşamasındaki performans değerleri Tablo 4.3'te verilmiştir.

Tablo 4.3. Modellerin test setindeki hata ölçüm parametreleri sonuçları.

Kullanılan Algoritma	R2	MSE	MAE	RMSE
LR	0,854693	3E+08	12261,911	110,73352
DTR	0,938990	1E+08	4059,746	63,71614
KNR	0,965149	8E+07	3212,579	56,67962
RFR	0,969421	7E+07	3626,203	60,21796
GBR	0,927065	2E+08	9130,024	95,55116

Algoritmaların başarılı eğitim süreci sonrasında normal veriseti üzerindeki test sonuçları da oldukça yüksek performans ile sonuçlanmıştır. Algoritmalara ait tahmin grafiğine Şekil 4.1'de yer verilmiştir. Parametre sonuçlarını doğrular şekilde gerçek sonuçlara çok yakın grafikler elde edilmiştir. Herhangi bir anomali barındırmayan ve yeterli eğitim verisetine sahip algoritmalar için beklendik sonuçlar alınmıştır.



Şekil 4.1. Algoritmalara ait tahmin grafiği.

Yüksek başarı oranıyla eğitilen modeller içerisinde anomali/siber saldırıların bulunduğu veri kümesi 3 üzerinde uygulanmıştır. Eğitim süresinde algoritmaların karşılaşmadıkları anormal durumlar modellerin çok farklı sonuçlar vermesine neden olmuştur. Anomalilere verilen anormal tepkiler modellerin hata parametreleri sonuçlara yansımış ve eğitim sürecine oranla çok kötü sonuçlar elde edilmiştir. Bu sonuçlara Tablo 4.4'te yer verilmiştir. Tablo 4.5. ile bu sonuçlar karşılaştırıldığında veri kümesi 3'ün veri kümesi 2'den farklı olduğu söyleyebiliriz. Algoritmaların parametre sonuçları farklı verisetlerine uygulandığında kabul edilir bir farktan fazlasına sahiptir. Örneğin, tabloda da görüldüğü gibi GBR parametresi test sürecinde R^2 değeri 0,93 iken veri seti 3'te 0,29 değerine sahiptir. Bu sonuçlarla modelimizin başarılı olduğunu kabul ederek veri seti 3 içerisindeki anomalileri tespit etmeye çalışıyoruz.

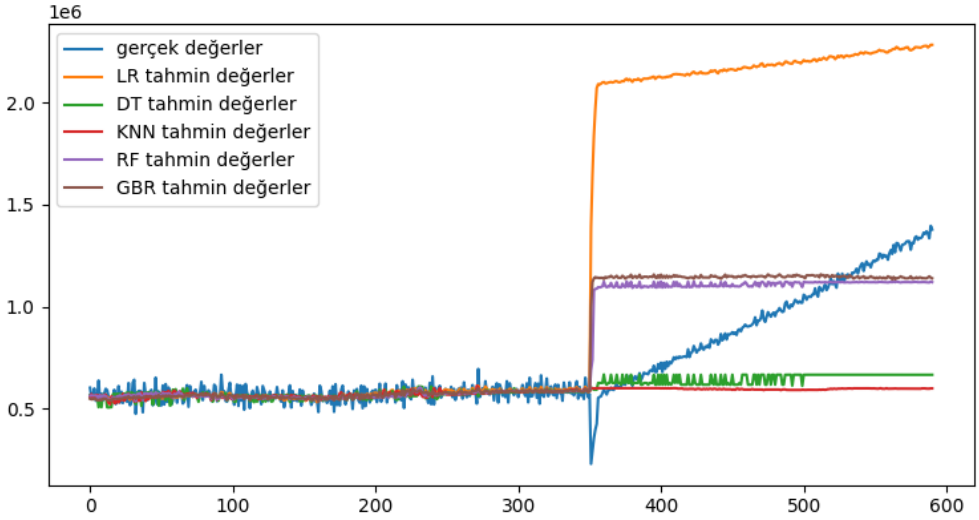
Tablo 4.4. Modellerin veri kümesi 3 üzerinde hata ölçüm parametreleri sonuçları.

Kullanılan Algoritma	R2	MSE	MAE	RMSE	MAPE
LR	-9,67495	6E+11	515211,99446	717,78269	62,77042
DTR	0,01269	6E+10	144583,15044	380,24091	15,39102
KNR	-0,26147	7E+10	162505,16509	403,11929	17,07713
RFR	0,42525	3E+10	112572,77625	335,51867	16,02271
GBR	0,28806	4E+10	122003,06380	349,28937	17,60955

Eğitim ve test aşamasında oldukça başarılı sonuçlar veren algoritmalar anomali barındıran veri seti üzerindeki aynı sonucu gösterememiştir ki bu beklenen durumdur. Bu kadar yüksek başarı elde eden algoritmaların sonuçlardan bu kadar uzaklaşması veri setinin içeresinde anomalileri doğrular niteliktedir (Şekil 4.2). Sisteme yapılan siber saldırılar anomali olarak adlandırılmaktadır. Eğitim verisetimizde anomali değerler olmadığından bir sınıflandırma işlemi yaparak anomali tespit etmemiz mümkün değildir. Bu durumda anomalileri tespit etmek için belirli bir eşik değeri(threshold) belirledik. Eşik değerleri belirlenirken model üzerindeki hassasiyet göze alınmalıdır. Eşik değeri belirlenirken sistemin özelliği ve hata toleransı göz önünde bulundurulmalıdır. Modelin tahmini ile gerçekleşen mevcut durum arasındaki fark bu eşik değerini aştığındaki noktalar anomali olarak işaretlenir.

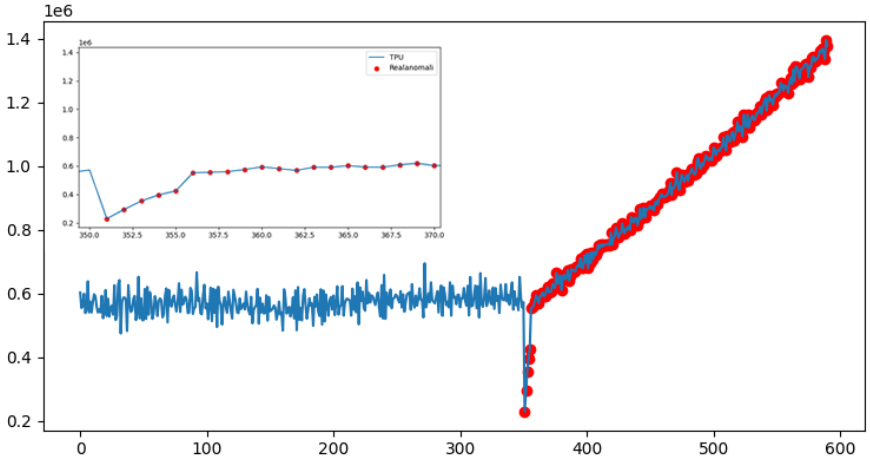
Literatürde yapılan çalışmalarda ortamda çok fazla düğüm bulunması durumunda optimum threshold değer ifadesini veren bir fonksiyon belirlenememiştir. Her threshold için precision, recall değerlerini hesaplayıp F1 skorunu maksimum yapan thresholdu seçmek bir yöntem olarak kabul edilmektedir. Veri kümesi 3 içerisindeki anomali değerlerini belirlemek için eşik değerini 0,7 olarak belirledik. Bu değer algoritmamızın tahmini ile mevcut durum arasında 0,7'den daha büyük bir fark olması burada anormallik olduğuna işarettir. Bu aynı zamanda yüksek bir performansa sahip algoritmaların mevcut sistem üzerinde 0,7'den daha büyük bir hatası kabul edilemez de demektir. Zaman serisi içerisinde belirli bir zamanda enjekte edilen siber saldırıların belirlenmesine modelin kendi değerleri arasındaki sapma bilgisinden yararlanmak her zaman sonuç vermeyebilir. Çünkü kötü niyetli kullanıcıların yaptıkları bu siber saldırılar bazen normal davranış gösterebilmektedir. Zaman serisi incelendiğinde indis değeri 351 dahil ve sonrasında modele saldırı gerçekleştirilmiştir. Bu indis değerinde sistem üzerindeki anormallik gözle gözlemlenebilmiş fakat 357.

indis değerinde saldırı devam etmesine rağmen anomaliler normal davranış göstermiştir (Şekil 4.2). Bu sonuçla saldırının normal davranış sergileyebileceği bu sistem üzerinde ispatlanmıştır.



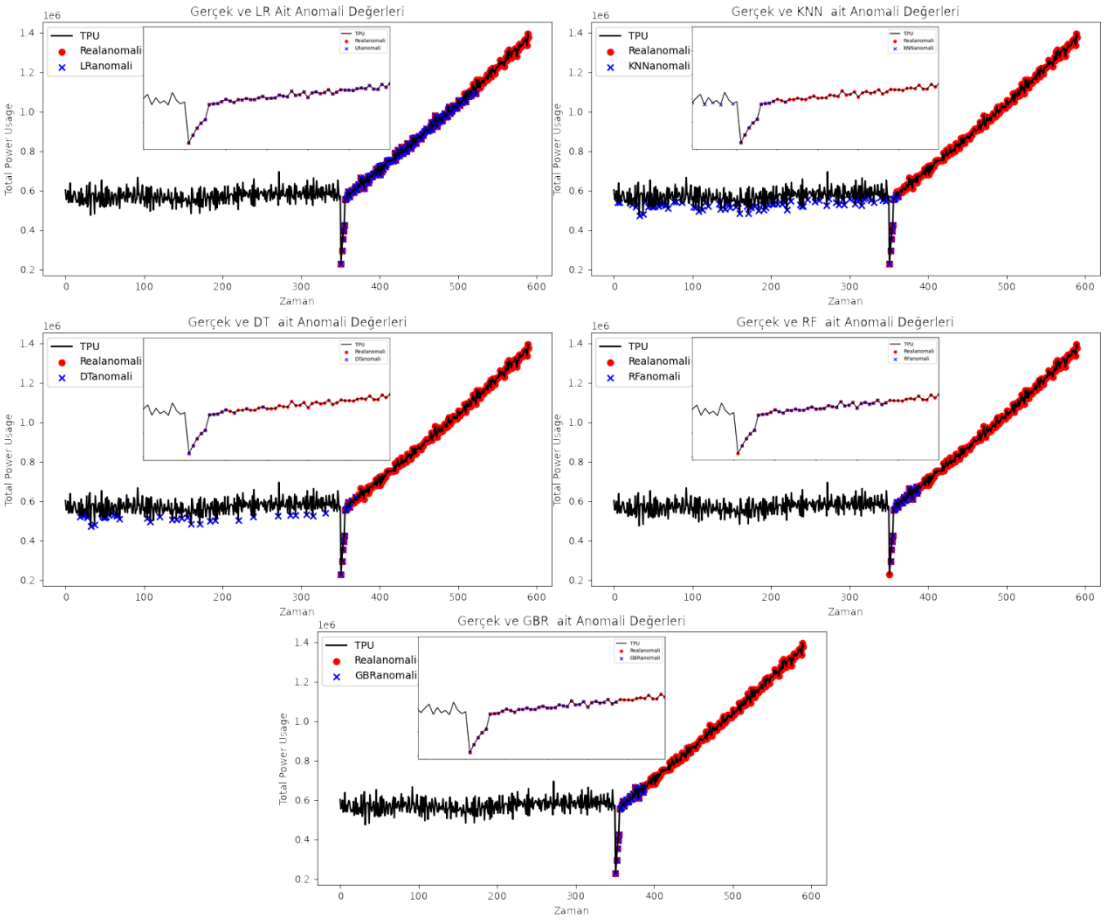
Şekil 4.2. Kullanılan modellerin anomalilere verdikleri tepkiler.

Modellerin karışıklık matrisi üzerinde karşılaştırılması işlemi yapabilmemiz için gerçek anomali ve gerçek normal değerlere ihtiyaç vardır. Simülasyon sonucunda ve gerçekleştirilen saldırı sonrasında gerçekleşen duruma Şekil 4.3'te yer verilmiştir. Şekil 4.3'te de görüldüğü gibi sisteme zaman serisine ait 351. indiste saldırı enjekte edilmiştir. Ve simülasyon sonlanana kadar bu saldırı devam etmiştir. Bu bilgiler ışığında bizim algoritmalarımızdan beklediğimiz sonuç saldırı zamanından sonra anormal durumu fark edip tepkilerini sonuca yansıtmalarıdır.



Şekil 4.3. Gerçek anomali değerleri.

Kullandığımız beş farklı makine öğrenmesinin anomali olarak tespit ettikleri noktalar Şekil 4.4'te verilmiştir. Algoritma sonuçlarını incelediğimizde KNR ve DTR algoritmaları siber saldırının sisteme enjekte edilmesinden önce zaman serisinin tahmin işleminde 0,7'den büyük hatalara sahip olduğundan bazı noktaları anomali olarak değerlendirmiştir ve kötü bir performans oluşturmuştur. LR, RFR ve GBR algoritmaları ise normal verileri doğru bir şekilde sınıflandırırken saldırı gerçekleşmesinin ardından bazı anomalileri sınıflandırmada zorluk yaşamıştır. LR, RFR ve GBR algoritmaları anomali ve normal veri sınıflandırmasında mevcut etiketsiz veriseti üzerinde diğer algoritmalara daha iyi sonuçlar vermiştir.



Şekil 4.4. Algoritmalar tarafından anomali olarak tespit edilen noktalar.

Elde ettiğimiz sonuçlar ile oluşturulan F ölçütü ve karışıklık matrisine göre sonuçlara sırasıyla Tablo 4.5 ve 4.6'da yer verilmiştir. Sonuçları incelediğimizde KNR ve DTR algoritmaları pozitif değerleri doğru sınıflandıramamasından dolayı oldukça düşük sonuçlar vermiştir. LR diğer algoritmalara göre çok yüksek doğruluk oranına sahipken RFR ve GBR benzer sonuçlar vermiştir. Algoritmaların bazıları yüksek sonuç

vermesine rağmen kabul edilebilir seviyede değildir. Bu çalışmada LR ve GBR algoritmaları ve veriseti üzerinde işlemlerden sonra mevcut durumdan daha yüksek doğruluk değerlerine ulaşmak hedeflenmektedir.

Tablo 4.5. F-ölçütüne göre modellerin sonuçları.

Kullanılan Algoritma	F1_Score
LR	0,81482
DTR	0,09825
KNR	0,05952
RFR	0,27338
GBR	0,21561

Tablo 4.6. Modellerin karışıklık matrisi sonuçları.

Kullanılan Algoritma	Accuracy	Sensitivity	Specificity	Precision
LR	0,87310	0,68750	1,0	1,0
DTR	0,56514	0,05833	0,91168	0,91168
KNR	0,46531	0,04167	0,75499	0,75499
RFR	0,65821	0,04717	1,0	1,0
GBR	0,64298	0,04525	1,0	1,0

Doğrusal regresyon modeli üzerinde yapılan çalışmalarda polinom regresyon ve farklı parametreler ile çalışmalar yapılmış fakat model performansında kabul edilebilir veya beklenen düzeyde bir artış gözlemlenememiştir. GBR algoritması üzerinde yapılan çalışmalara bir sonraki bölümde ayrıntılı olarak yer verilmiştir.

4.5. Geliştirilen Model Ve Parametreleri

GBR algoritmasının model üzerinde en uygun parametreleri belirlemek amacıyla model parametrelerinde değişiklik yapılıp mae hesaplanarak performansları karşılaştırılmıştır. “n_estimators” parametresi modellenecek ardışık ağaç sayısını temsil etmektedir. GBM için fazla sayıda ağaç olması modeli sağlamlaştırsa belirli bir noktadan sonra aşırı yükleme oluşturup modelin performansını olumsuz yönde etkileyebilir. Bu yüzden belirli öğrenme oranlarında denemeler yaparak belirlemek bu sorunu çözecektir. “max_leaf_nodes” parametresi bir ağaçtaki maksimum yaprak

sayısını ifade eder. Maksimum derinlik yerine tanımlanabilir. İkili olarak ağaç oluşturulduğundan n derinliğini temsil ettiği düşünürsek 2^n yaprak sayısı olarak hesaplanabilir. "learning_rate" her ağacın nihai sonuç üzerindeki etkisini belirler. GBM her ağacın çıktısını kullanarak güncellenen bir ilk tahmin ile başlayarak çalışan bir sistemdir. Öğrenme parametresi tahminlerdeki bu değişikliğin büyüklüğünü kontrol eder. Ağaç belirli özelliklere karşı dayanıklı hale getirir ve böylece iyi bir genelleme yapmasına izin verdiği için genellikle küçük değerler tercih edilir. Düşük değerler ise tüm ilişkileri modellemek için daha fazla sayıda ağaç gerektirecektir ve hesaplama açısından maliyeti arttıracaktır. Bu bilgiler göz önüne alındığında "n_estimators" parametresi 1, 2, 5, 10, 20, 50, 100, 200, 500 değerleri arasında, "max_leaf_nodes" parametresi 2, 5, 10, 20, 50, 100 değerleri arasında belirli öğrenme parametreleri ile hata ölçüm parametrelerine göre karşılaştırılarak en uygun seçim yapılmaya çalışılmıştır. Parametrelere göre elde edilen sonuçlar Şekil 4.5'te gösterilmiştir.

	param_n_estimators	param_max_leaf_nodes	param_learning_rate	mean_test_error	std_test_error
6	500	100	0.709894	6583.454285	272.544209
17	500	5	0.771785	6599.807176	220.661664
1	200	20	0.160519	7722.524216	184.852074
10	200	20	0.109889	8185.124949	181.154459
12	200	50	0.110585	8192.078659	191.210920
3	500	2	0.07502	10384.324846	220.711337
4	100	5	0.0351	10878.786057	167.743062
18	10	5	0.637819	10883.582846	252.114129
8	5	2	0.462636	16176.293886	317.631500
19	5	20	0.202432	17360.862419	176.779985
9	10	5	0.088556	20075.483792	214.737081
5	2	2	0.421054	23538.681158	305.531172
15	50	100	0.010904	24767.524657	185.489995
2	5	100	0.070357	28368.428209	231.439026
16	2	50	0.167568	28430.043992	203.776837
11	1	5	0.190477	32453.493831	185.559278
13	5	20	0.033815	33164.140597	217.156267
0	1	100	0.125207	34334.976069	211.454372
14	1	10	0.081715	35685.818450	239.087515
7	1	20	0.014937	37778.242720	292.292467

Şekil 4.5. Parametre değişikliklerine göre alınan sonuçlar.

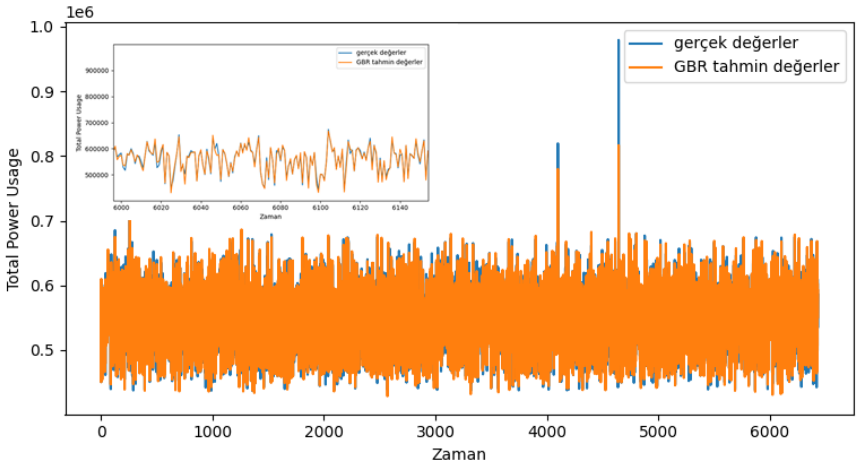
Şekil 4.5.'teki sonuçlar göz önüne alındığında en düşük hata oranına sahip parametreler GBR modeline uygulanmıştır. Değişiklik uygulanan GBR modeli bundan sonraki bölümlerde GBR* olarak ifade edilecektir. Model parametrelerinden sonra veriseti giriş parametreleri korelasyonel ilişki bakımından incelerek indirgenmeye çalışılmıştır. +0,95 ile -0,95'ten yüksek ilişki gösteren değişkenler azaltılarak 31'e kadar düşürülmüştür. Belirlenen parametrelerin verisetini tam anlamıyla tespit etmesi önem arz etmektedir. İlişki bakımından daha düşük benzerlik oranına sahip giriş parametrelerinin dahil edilmemesi model performansını olumsuz bir şekilde etkilemiştir. Bu yüzden farklı korelasyona sahip parametreler özgün kabul edilip direk sisteme dahil edilmiştir. Çıkış parametresi üzerinde benzer etkiye sahip giriş parametrelerinin azaltılması modelin yükünü azaltarak performansını arttıracaktır. Büyük verilerde aşırı öğrenme sorunu her zaman göz önünde bulundurulmalıdır. Fakat öz nitelik seçimi yapılırken verisetini tam anlamıyla temsil etmesi gerekmektedir. Öz nitelik seçiminde korelasyonel ilişki dışında derin öğrenme algoritmaları ve temel bileşen analizine sık sık başvurulmaktadır. Model ve veriseti işlemleri tamamlandıktan sonra elde edilen hata ölçüm parametrelerine ait sonuçları Tablo 4.7'de sunulmuştur. Model parametrelerinin ve veriseti işlemlerimiz sonucu olumlu şekilde etkilemiş ve oluşan hata değerlerinde düşüş gerçekleşmiştir.

Tablo 4.7. GBR* modelinin ait sonuçlar ve karşılaştırılması.

Kullanılan Algoritma	R2	MSE	MAE	RMSE
LR	0,85469	3,4E+08	12261,91	110,73352
GBR	0,92707	1,7E+08	9130,02	95,55116
GBR*	**0,96401**	**8,1E+07**	**6280,10**	**79,24706**

Modelin test sürecinde oluşan tahmin grafiğine Şekil 4.6.'da yer verilmiştir. Model gerçeğe çok yakın sonuçlar üretmiştir. Belirleme katsayısı yani R-kare bağımlı değişkenin değerinde farklılaşmayı açıklayabilmesine göre 0 ile 1 arasında değer alır ve 1 en yüksek sonucu ifade etmektedir. Modelimiz giriş parametrelerine bakarak bağımlı değişkenimizin tepkisi 0,96 oranında anlamlandırabilmiştir. Hata değerlerinde düşüş ile yapılan korelasyonel işlemlerin ve parametre değişikliğinin model üzerinde pozitif etki yarattığını söyleyebiliriz.

Modelimizin sistem için kabul edilebilir seviyede performans göstermesinin ardından siber saldırıların bulunduğu veri kümesi 3'e uyguladıktan sonra aynı eşik değeri üzerinden anomalileri tespit etmesini sağladık. GBR* algoritmasının F-ölçütüne göre sonucuna ve LR, GBR algoritması ile karşılaştırılmasına Tablo 4.8'de yer verilmiştir.

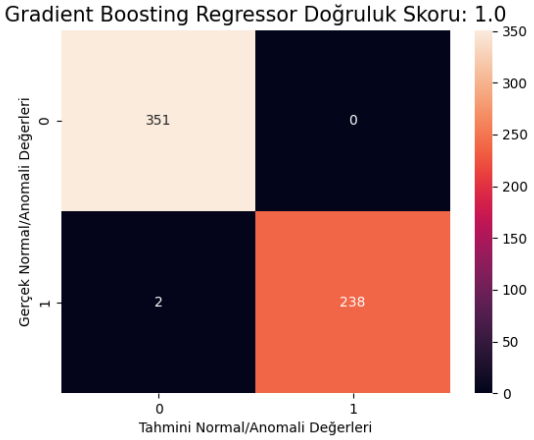


Şekil 4.6. Geliştirilen GBR* modeline ait tahmin grafiği.

Tablo 4.8. Geliştirilen modelin F-ölçütüne göre sonuçları ve karşılaştırılması.

Kullanılan Algoritma	F1_Score
LR	0,81482
GBR	0,21561
GBR*	**0,99582**

Belirlenen eşik değerinin üzerinde yapılan hata değerlerine sahip tahminlerin anomali ve diğerlerinin normal olarak sınıflandırılmasının ardından karışıklık matrisi oluşturulmuştur (Şekil 4.7).



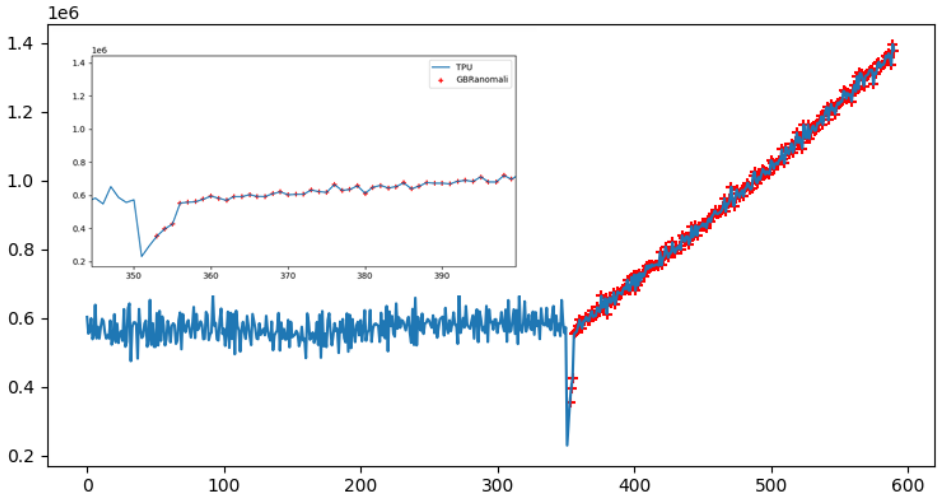
Şekil 4.7. Karışıklık matrisi sonuçları GBR*.

Karışıklık matrisi kullanılarak modelimizin hata değerleri ve hata türlerine ait bilgi sahibi olabiliriz. Karışıklık matrisi bilgileri kullanılarak elde edilen sonuçlara ve diğer algoritmalar ile karşılaştırılması Tablo 4.9'da sunulmuştur. Accuracy ve Sensitivity değerleri yükselmiş ve kritik altyapılarda kabul edilebilir şekilde sonuçlar alınmıştır.

Tablo 4.9. Geliştirilen modelin karışıklık matrisi sonuçları ve karşılaştırılması.

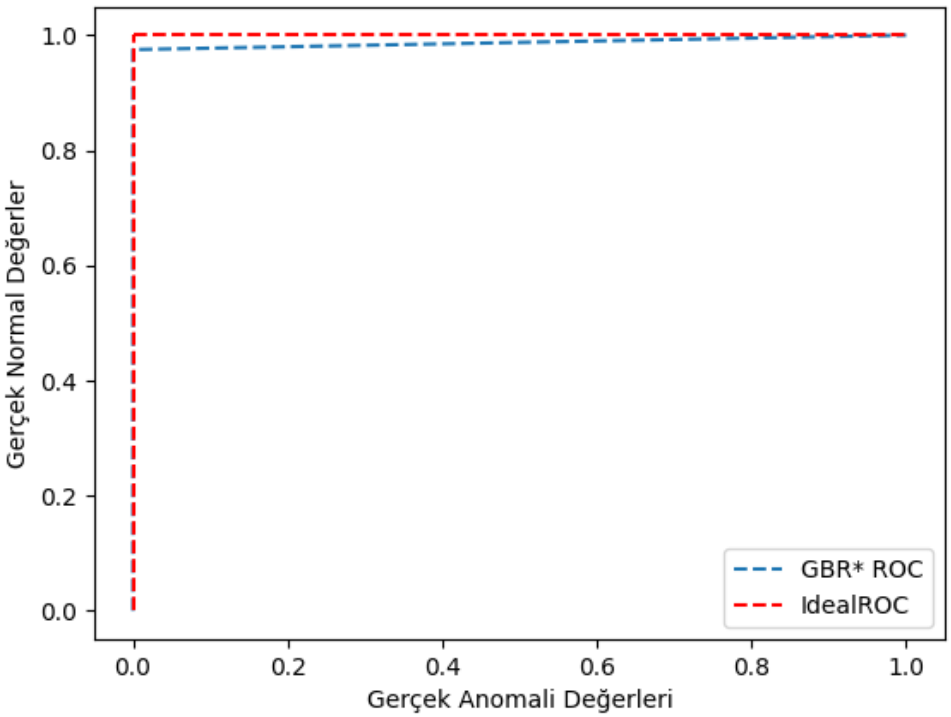
Kullanılan Algoritma	Accuracy	Sensitivity	Specificity	Precision
LR	0,87310	0,68750	1,0	1,0
GBR	0,64300	0,04525	1,0	1,0
GBR*	**1,0**	**0,99167**	**1,0**	**1,0**

Şekil 4.8.'de modelimizin anomali olarak belirlediği noktalar gösterilmiştir.



Şekil 4.8. GBR* modelinin anomali olarak tespit ettiği noktalar.

Karışılık matrisinden elde ettiğimiz sonuçlar tatmin edici seviyede olsa da daha iyi sonuçlar veren ROC eğrisinden yararlandık. Modellerin karşılaştırılmasında doğruluk değerine göre benzer sonuçlar alsak da AUC'a göre farklı sonuçlar elde edilmiştir. Ve eğri altında kalan alanın yani AUC değerinin oldukça yüksek olduğunu tespit ettik. İdeal ROC eğrisine yakın sonuç veren modelimizin geçerliliği mevcut veri seti üzerinde ispatlanmıştır. İdeal ROC eğrisi ve modelimize ait ROC eğrisi Şekil 4.9'da verilmiştir.



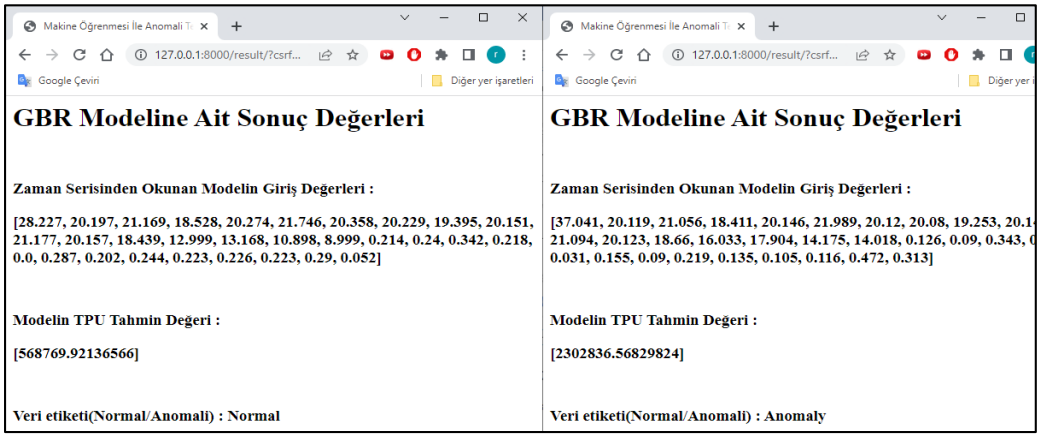
Şekil 4.9. GBR* ve ideal ROC eğrisi.

4.6. Web Tabanlı Anomali Tespit Uygulaması

Anomali tespiti konusunun diğer önemli noktalarından biri de gerçek zamanlı olarak durumların zaman serisi üzerinde tespit edilmesidir. Bu amaç doğrultusunda web tabanlı çalışan bir uygulama gerçekleştirdik. Gerçekleştirilen projeye bir önceki bölümde anlatılan GBR* algoritması entegre edilmiştir. Projeye ait veritabanına içinde siber saldırıların bulunduğu veriler yerleştirilmiştir. Basit bir giriş ekranından zaman serisine ait ilgili veri bilgisine ulaşım imkânı sağlanmıştır. Proje üzerinde bu verilerin sensörler yardımıyla okunan anlık veri akışı olarak değerlendirilmiştir. Projeye ait giriş sayfasına şekil 4.10'da yer verilmiştir.

Şekil 4.10. Web tabanlı projeye ait giriş sayfası.

Metin kutusuna girilen değer ile veritabanı üzerinde gerçekleştirilen sorgular sayesinde veriler kontrol edilerek sunulmaktadır. Sunulan verilen geliştirilen GBR* modeline giriş parametreleri olarak verilmektedir ve model sonucunda oluşan tahmin değeri belirli bir threshold değeri ile kontrol edilmektedir. Kontrol sonucuna ilgili zaman serisine ait veri normal veya anormal olarak kullanıcıya sunulmaktadır. Projeye ait 1. ve 400. verileri ait sonuç ekranına şekil 4.11'de yer verilmiştir.



Şekil 4.11. Web tabanlı projeye ait sonuç ekranı.

Web tabanlı gerçekleştirilen uygulama sayesinde verilerin anlık olarak okunması ile sistem üzerinde gerçekleştirilebilecek siber saldırılar veya anormal durumların gecikme yaşanmadan tespit edilebilecektir. Bu tür durumların tespitinde zaman en önemli kriterler arasında yer almaktadır. Sistem üzerindeki olumsuz durumların tespit edilmesinde yaşanabilecek gecikmeler oluşabilecek olumsuz durumların büyüklüğünü etkilemektedir. Projenin gerçekleştirilmesinde gradyan artırma modeli kullanılarak eğitim jupyter notebook 6.5.2 sürümü üzerinde gerçekleştirilmiştir. Visual studio code 17.5 sürümü kullanılarak oluşturulan model projenin içine aktarılmıştır. Sistem özellikleri Intel Core i7-10750H CPU 2.60GHz 2.59 GHz işlemci ve nVIDIA GeForce GTX1650 Ti 4GB GDDR6 128-Bit DX12 ekran kartı ile gerçekleştirilmiştir. Model python 3.9.15 sürümü ile gerçekleştirilmiştir. SQLiteStudio 3.4.4 sürümü kullanılmıştır.

5. SONUÇLAR VE ÖNERİLER

HVAC sisteme ait zaman serisi üzerinde anomali tespit amacıyla 5 farklı makine öğrenmesi yöntemi ile çalışmalar yapılmıştır. Bu çalışmalarda parametre seçiminin dışında giriş değişkenleri üzerinde yapılacak indirgeme işlemleri modelin aşırı yüklenmesine önüne geçerek performansının arttırılabileceği gösterilmiştir. Büyük verilerde modeli örnekleyecek düzgün yöntemlerin seçilmesi oldukça önemlidir.

Bunun sonucunda veri kümesi 3'teki zaman serisi üzerinde yapılan 4 farklı gruba ait 16 farklı siber saldırıyı başarılı bir şekilde tahmin etmiştir.

Bu tez çalışmasında sadece HVAC sisteme ait bir veri seti üzerinde çalışmalar gerçekleştirilmiştir. Farklı veri setlerinde üzerinde yapılacak çalışmalar ile elde edilen sonuçlar hakkında daha genel ve net ifadeler elde edilebilir. Ayrıca bundan sonraki yapılacak çalışmalarda gerçekleştirilecek ufak bir prototip üzerinde sensörden gelen verilerin okunması ile sisteme enjekte edilen siber saldırıların tespit edilmesine dayanan bir model niteliğinde uygulama gerçekleştirilebilir.

Yapılan tez çalışmasının literatüre katkısını aşağıdaki şekilde sıralanabilir:

- 5 farklı makine öğrenmesi algoritmalarının zaman serileri üzerindeki anomali tespiti üzerine performansları gözlemlenmiştir.
- Korelasyonel ilişki ile giriş ve çıkış parametrelerinin model sonucuna etkisi değerlendirilmiştir.
- Anomali tespiti ve zaman serileri üzerinde araştırmalar yapılmış ve bu alandaki diğer çalışmalara kaynaklık edebilecek bir çalışmadır.
- Çok değişkenli zaman serilerinde yapılacak ölçeklendirme işlemlerinin modeller üzerinde etkisi gözlemlenmiştir ve örnek oluşturmuştur.
- Django ile web tabanlı anomali tespit uygulamalarına performans değerlendirme çalışmalarına örnek teşkil edilebilir.

KAYNAKLAR

[1] J. A. Leech, W. C. Nelson, R. T Burnett, S. Aaron, and M. E. Raizenne, "It's about time: a comparison of canadian and american time–activity patterns," Journal of Exposure Science and Environmental Epidemiology, vol. 12, no. 6, p. 427, 2002.

[2] S. Wendzel, J. Tonejc, J. Kaur, and A. Kobekova, Cyber security of smart buildings. Wiley, 2017.

[3] K. Zetter, "Researchers hack building control system at Google australia office," Wired. com, available at https://www.wired.com/2013/05/googles-control-system-hacked (accessed 9th June, 2017), 2013.

[4] B. Krebs, "Target hackers broke in via hvac company," Krebs on Security, 2014.

[5] Markets and Markets, "Smart hvac controls market by product type, components, application, operation & geography-analysis and forecast to 2014-2020," 2014.

[6] J. Vijayan, "With the internet of things, smart buildings pose big risk," Computer World, 2014.

[7] A. J. Fox. 1972. Outliers in time series. J. Roy. Stat. Soc.: Ser. B (Methodol.) 34, 3 (1972), 350–363.

[8] A. Blázquez-García, A. Conde, U. Mori, and J. A. Lozano, ''A review on outlier/anomaly detection in time series data,'' 2020, arXiv:2002.04236. [Online]. Available: http://arxiv.org/abs/2002.04236

[9] A. Carreño, I. Inza, and J. A. Lozano. 2020. Analyzing rare event, anomaly, novelty and outlier detection terms under the supervised classification framework. Artific. Intell. Rev. 53, 5 (2020), 3575–3594.

[10] A. Keliris, H. Salehghaffari, B. Cairl, P. Krishnamurthy, M. Maniatakos, and F. Khorrami, ''Machine learning-based defense against process-aware attacks on industrial control systems,'' in Proc. IEEE Int. Test Conf. (ITC), Nov. 2016, pp. 1–10, doi: 10.1109/test.2016.7805855.

[11] K. Paridari, A. E.-D. Mady, S. La Porta, R. Chabukswar, J. Blanco, A. Teixeira, H. Sandberg, M. Boubekeur, Cyber-physical-security framework for building energy management system, in: Cyber Physical Systems (ICCPS), 2016 ACM/IEEE 7th International Conference on, IEEE, 1–9, 2016

[12] P.M. Van Every, M. Rodriguez, C. Birk Jones, A.A. Mammoli, M. Martínez Ramón Advanced detection of HVAC faults using unsupervised SVM novelty detection and Gaussian process models Energ. Buildings, 149 (2017), pp. 216-224, 10.1016/j.enbuild.2017.05.053

[13] K. Paridari, N. OMahony, A. E.-D.Mady, R. Chabukswar,M. Boubekeur, and H. Sandberg, “A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration,” Proc. IEEE, vol. 106, no. 1, pp. 113–128, 2017.

[14] C. Valli, M. N. Johnstone, M. Peacock, and A. Jones, “Bacnet - bridging the cyber physical divide one hvac at a time,” in 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), 2017, pp. 1–6.

[15] C. B. Jones and C. Carter, ‘‘Trusted interconnections between a centralized controller and commercial building HVAC systems for reliable demand response,’’ IEEE Access, vol. 5, pp. 11063–11073, 2017.

[16] S. Wang, J. Xing, Z. Jiang et al., “A decentralized sensor fault detection and self-repair method for HVAC systems,” Building Services Engineering Research and Technology, vol. 39, no. 6, pp. 667–678, 2018. [Google Scholar] [CrossRef]

[17] M. Guirguis, A. Tahsini, K. Siddique, C. Novoa, J. Moore, C. Julien, and N. Dunstatter. Bloc: A game theoretic approach to orchestrate cps against cyber attacks. In 2018 IEEE Conference on Communications and Network Security (CNS), pages 1–9. IEEE, 2018.

[18] A. Patil, V. Kamuni, A. Sheikh, S. Wagh, and N. Singh, “A machine learning approach to distinguish faults and cyberattacks in smart buildings,” in 2019 9th International Conference on Power and Energy Systems (ICPES). IEEE, 2019, pp. 1–6.

[19] S. D. Roy and S. Debbarma, ‘‘Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid,’’ IEEE Syst. J., vol. 14, no. 2, pp. 2023–2031, Jun. 2019.

[20] A. Sheikh, V. Kamuni, A. Patil, S. Wagh, and N. Singh, “Cyber attack and fault identification of hvac system in building management systems,” 2019 9th international conference on power and energy systems (ICPES), IEEE (2019), pp. 1-6.

[21] E. Novikova, M. Bestuzhev, and I. Kotenko, “Anomaly detection in the HVAC system operation by a RadViz based visualizationdriven approach,” in Comput. Secur., 2019, pp. 402–418.

[22] Y. Xu, C. Yan, J. Shi, Z. Lu, X. Niu, Y. Jiang, et al., "An anomaly detection and dynamic energy performance evaluation method for hvac systems based on data mining", Sustainable Energy Technologies and Assessments, vol. 44, pp. 101092, 2021. [Google Scholar] [CrossRef]

[23] E. Novikova, M. Bestuzhev, “Exploration of the Anomalies in HVAC Data Using Image Similarity Assessment,” In Proceedings of the 2020 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 8–11 June 2020; pp. 1–4. [Google Scholar]

[24] E. Novikova, M. Bestuzhev, and A. Shorov, “The Visualization-Driven Approach to the Analysis of the HVAC Data,” in Studies in Computational Intelligence vol. 868, ed, 2020, pp. 547-552.

[25] K. Filus, J. Domanska, and E. Gelenbe, “Random neural network for ´ lightweight attack detection in the iot,” in Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems. Springer, 2020, pp. 79–91.

[26] Novikova, E., Belimova, P., Dzhumagulova, A., Bestuzhev, M., Bezbakh, Y., Volosiuk, A., Balkanskii, A., Lavrov, A.: Usability assessment of the visualization-driven approaches to the HVAC data exploration. In: CEUR Workshop Proceedings (2020). https://doi.org/10.51130/ graphicon-2020-2-3-17.

[27] Gao G, Li J, Wen Y (2020) Deepcomfort: energy-efcient thermal comfort control in buildings via reinforcement learning. IEEE Internet Things J 7(9):8472–8484

[28] Maitreyee Dey, Soumya Prakash Rana, Sandra Dudley, Smart building creation in large scale HVAC environments through automated fault detection and diagnosis, Future Generation Computer Syst. 108 (2020) 950–966.

[29] Li Y, Tong Z (2021) Model predictive control strategy using encoder-decoder recurrent neural networks for smart control of thermal environment. J Build Eng 42:103017

[30] Nur Imtiazul Haque, Mohammad Ashiqur Rahman, and Hossain Shahriar. Ensemble-based efficient anomaly detection for smart building control systems. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pages 504–513. IEEE, 2021.

[31] Chakraborty, S.; Onuchowska, A.; Samtani, S.; Jank, W.; Wolfram, B. Machine Learning for Automated Industrial IoT Attack Detection: An Efficiency-Complexity Trade-off. ACM Trans. Manag. Inf. Syst. 2021, 12, 1–28. [Google Scholar] [CrossRef]

[32] Aaron W Werth and Thomas H Morris. 2020. Prototyping PLCs and IoT Devices in an HVAC Virtual Testbed to Study Impacts of Cyberattacks. In International Congress on Information and Communication Technology. Springer, 612–623.

[33] Sudharsan, B., Sundaram, D., Patel, P., Breslin, J.G., Ali, M.I.: Edge2guard: Botnet attacks detecting offline models for resource-constrained iot devices. In: 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops). pp. 680–685. IEEE (2021)

[34] Fu Y, O’Neill Z, Yang Z, Adetola V, Wen J, Ren L, et al. Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings. Appl Energy 2021;303: 117639. https://doi.org/10.1016/j.apenergy.2021.117639.

[35] Shichao Xu, Yangyang Fu, Yixuan Wang, Zheng O’Neill, and Qi Zhu. 2021. Learning-based framework for sensor fault-tolerant building HVAC control with model-assisted learning. In Proceedings of the 8th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation. 1–10.

[36] Su, Q.; Li, S.; Gao, Y.; Huang, X.; Li, J. Observer-based detection and reconstruction of dynamic load altering attack in smart grid. J. Frankl. Inst. 2021, 358, 4013–4027. [Google Scholar] [CrossRef]

[37] COSHATT, Stephen J., et al. Fault and Attack Detection and Diagnosis by Analysis of Electrical Waveforms of Power Networks. In: 2022 IEEE Aerospace Conference (AERO). IEEE, 2022, 1-9.

[38] Elyoussoufi, S., Mazouzi, M.,Cherrafi ,A., Tamasna,E.M., TRIZ-ISHIKAWA diagram, a new tool for detecting influencing factors: a case study in HVAC business, Proceedings of the International Conference on Industrial Engineering and Operations Management, 2022, 7-10.

[39] Y. Jiang, S. Wu, H. Yang, H. Luo, Z. Chen, S. Yin, O. Kaynak, Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework, IEEE Trans. Syst. Man Cybern.: Syst. Google Scholar

[40] Cash, M., C. Morales, S. Wang, X. Jin, A. Parlato, Q.Z. Sun and X. Fu, On False Data Injection Attack against Building Automation Systems. 2022, arXiv.

[41] Li, G., Yang, Z., Fu, Y., Ren, L., O'Neill, Z., & Parikh, C. (2022). Development of a hardware-In-the-Loop (HIL) testbed for cyber-physical security in smart buildings. arXiv preprint arXiv:2210.11234.

[42] Borda, D.; Bergagio, M.; Amerio, M.; Masoero, M.C.; Borchiellini, R.; Papurello, D. Development of Anomaly Detectors for HVAC Systems Using Machine Learning. Processes 2023, 11, 535. [Google Scholar] [CrossRef]

[43] Z. Wang, T. Parkinson, P. Li, et al., The Squeaky wheel: machine learning for anomaly detection in subjective thermal comfort votes[J], Build. Environ. 151 (2019) 219–227.

[44] Wang, D.; Wang, X.; Zhang, Y.; Jin, L. Detection of power grid disturbances and cyber-attacks based on machine learning. J. Inf. Secur. Appl. 2019, 46, 42–52. [Google Scholar] [CrossRef]

[45] Y. Himeur, A. Elsalemi, F. Bensaali, A. Amira, Smart power consumption abnormality detection in buildings using micro-moments and improved K-nearest neighbors, Int. J. Intell. Syst. (2020) 1–25.

[46] A. Parizad, C.J. Hatziadoniu, Cyber-attack detection using principal component analysis and noisy clustering algorithms: a collaborative machine learning-based framework, IEEE Trans. Smart Grid 13 (No. 6) (2022) 4848–4861.

[47] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.- W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," International Journal of Electrical Power & Energy Systems, vol. 91, pp. 230–240, 2017.

[48] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," IEEE Trans. Ind. Informat., vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[49] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 216–226, Jan. 2015.

[50] G. M. Messinis, A. E. Rigas, and N. D. Hatziargyriou, “A hybrid method for non-technical loss detection in smart distribution grids,” IEEE Trans. Smart Grid, vol. 10, no. 6, pp. 6080–6091, Nov. 2019.

[51] Hasan M., Toma R.N., Nahid A.-A., Islam M., Kim J.-M., et al. Electricity theft detection in smart grid systems: a CNN-LSTM based approach Energies, 12 (17) (2019), p. 3310

[52] Bunning F, Huber B, Heer P, Aboudonia A, Lygeros J. Experimental demonstration of data predictive control for energy optimization and thermal comfort in buildings211. Energy and Buildings; 2020, 109792

[53] Amirhossein Ahmadi, Mojtaba Nabipour, Saman Taheri, Behnam Mohammadi-Ivatloo, Vahid Vahidinasab, A new false data injection attack detection model for cyberattack resilient energy forecasting, IEEE Trans. Ind. Inf. (2022) 1, http://dx.doi.org/10.1109/TII.2022.3151748.

[54] S. Taheri, A. Ahmadi, B. Mohammadi-Ivatloo, S. Asadi, Fault detection diagnostic for HVAC systems via deep learning algorithms, Energy Build. 250 (2021) 111275, https://doi.org/10.1016/j.enbuild.2021.111275.

[55] R. Punmiya and S. Choe, “Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing,” IEEE Trans. Smart Grid, vol. 10, no. 2, pp. 2326–2329, Mar. 2019.

[56] R. Razavi, A. Gharipour, M. Fleury, and I. J. Akpan, “A practical featureengineering framework for electricity theft detection in smart grids,” Appl. energy, vol. 238, pp. 481–494, Mar. 2019.

[57] Khan, I.U.; Aslam, N.; AlShedayed, R.; AlFrayan, D.; AlEssa, R.; AlShuail, N.A.; Al Safwan, A. A Proactive Attack Detection for Heating, Ventilation, and Air Conditioning (HVAC) System Using Explainable Extreme Gradient Boosting Model (XGBoost). Sensors 2022, 22, 9235. [Google Scholar] [CrossRef]

[58] Elnour, M., Meskin, N., Khan, K., & Jain, R. (2021). Application of data-driven attack detection framework for secure operation in smart buildings. Sustainable Cities and Society, 69, 102816.

[59] Bode G, Thul S, Baranski M, Müller D. Real-world application of machinelearning-based fault detection trained with experimental data. Energy May 2020; 198:117323. https://doi.org/10.1016/j.energy.2020.117323.

[60] Mahesh, B. Machine Learning Algorithms-A Review. Int. J. Sci. Res. 2020, 9, 381–386. 65

[61] Murphy, K. P. (2012). Machine Learning: A Probabilistic Perspective. In The MIT Press Cambridge, Massachusetts London, England. 66

[62] James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). An Introduction to Statistical Learning with Applications in R. Springer.

[63] Kılınç, D., Başeğmez, D. (2018). Uygulamalarla Veri Bilimi, 1.Baskı, Abaküs Yayınları, İstanbul, Türkiye.

[64] Frank, H., & Kotthoff, L. (2019). Automatic machine learning: methods, systems, 104 challenges. Springer.

[65] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM Comput. Surv., vol. 41, no. 3, pp. 1–58, 2009.

[66] Ratanamahatana, C., Lin, J., Gunopulos, D., Keogh, E., Vlanchos, M., & Das, G. (2010). Mining time series data. Data mining and knowledge discovery handbook, (pp. 1069– 1103).

[67] Fu, T.-C. (2011). A review on time series data mining. Engineering Applications of Artificial Intelligence, 24(1), 164–181.

[68] Esling, P., & Agon, C. (2012). Time series data mining. ACM Computing Surveys (CSUR), 45(1), 1–34.

[69] X. Song, M. Wu, C. Jermaine, and S. Ranka, “Conditional anomaly detection,” IEEE Trans. Knowl. Data Eng., vol. 19, no. 5, pp. 631–645, May 2007.

[70] Huang Z, “Extensions to the k-means algorithm for clustering large data sets with categorical values,” Data Mining and Knowledge Discovery, Vol.2, pp:283–304, 1998.

[71] Sun Shibao, Qin Keyun,”Research on Modified k-means Data Cluster Algorithm”I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” Computer Engineering, vol.33, No.13, pp.200– 201,July 2007.

[72] Fahim A M,Salem A M,Torkey F A, “An efficient enhanced k-means clustering algorithm” Journal of Zhejiang University Science A, Vol.10, pp:1626-1633,July 2006.

[73] Yuan F, Meng Z. H, Zhang H. X and Dong C. R, “A New Algorithm to Get the Initial Centroids,” Proc. of the 3rd International Conference on Machine Learning and Cybernetics, pp. 26–29, August 2004.

[74] Sun Jigui, Liu Jie, Zhao Lianyu, “Clustering algorithms Research”,Journal of Software ,Vol 19,No 1, pp.48-61,January 2008.

[75] Na, S., Xumin, L. & Yong, G. Research on k-means clustering algorithm: an improved k-means clustering algorithm. in 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, 63–67 (IEEE, 2010).

[76] K.A.Abdul Nazeer, M.P.Sebastian, “Improving the Accuracy and Efficiency of the k-means Clustering Algorithm”,Proceeding of the World Congress on Engineering, vol 1,london, July 2009.

[77] Podgorelec, V.; Kokol, P.; Stiglic, B.; Rozman, I. Decision Trees: An Overview and Their Use in Medicine. J. Med. Syst. 2002, 26, 445−463.

[78] Quinlan, J. R., C4.5: Programs for Machine Learning, Morgan Kaufmann, San Francisco, 1993.

[79] Yoav Freund and Robert E. Schapire. A decision-theoretic generalization of on-line learning and an application to boosting. Journal of Computer and System Sciences, 55(1):119–139, August 1997.

[80] Schapire, R. E. The Boosting Approach to Machine Learning: An Overview. In Nonlinear Estimation and Classification; Springer: New York, 2003.

[81] A. Natekin and A. Knoll, ‘‘Gradient boosting machines, a tutorial,’’ Frontiers Neurorobotics, vol. 7, no. 7, pp. 1–21, 2013.

[82] Friedman, J. H. (2001). Greedy function approximation: a gradient boosting machine. Annals of statistics, 1189-1232.

[83] R. Bekkerman. The present and the future of the kdd cup competition: an outsider's perspective.

[84] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12:2825–2830, 2011.

[85] G. Ridgeway. Generalized Boosted Models: A Guide to the GBM Package. Update, 1(1):1–12, 2007.

[86] M. Greenwald and S. Khanna. Space-efficient online computation of quantile summaries. In Proceedings of the 2001 ACM SIGMOD International Conference on Management of Data, pages 58–66, 2001.

[87] Q. Zhang and W. Wang. A fast algorithm for approximate quantiles in high speed data streams. In Proceedings of the 19th International Conference on Scientific and Statistical Database Management, 2007.

[88] Chen, T., He, T., Benesty, M., Khotilovich, V., Tang, Y., Cho, H., ... & Zhou, T. (2015). Xgboost: extreme gradient boosting. R package version 0.4-2, 1(4), 1-4.

[89] Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., ... & Liu, T. Y. (2017). Lightgbm: A highly efficient gradient boosting decision tree. Advances in neural information processing systems, 30.

[90] Chen, C.; Zhang, Q.; Ma, Q.; Yu, B. LightGBM-PPI: Predicting protein-protein interactions through LightGBM with multi-information fusion. Chemom. Intell. Lab. Syst. 2019, 191, 54–64.

[91] Sun, X.; Liu, M.; Sima, Z. A novel cryptocurrency price trend forecasting model based on LightGBM. Financ. Res. Lett. 2018.

[92] Liudmila P, Gleb G, Aleksandr V, Anna Veronika D, Andrey G. Catboost: unbiased boosting with categorical features. In S. Bengio, H. Wallach, H. Larochelle, K. Grauman, N. Cesa-Bianchi, and R. Garnett, editors, Advances in Neural Information Processing Systems 31, 2018; pages 6638–6648. Curran Associates, Inc.

[93] Wu, T.; Zhang, W.; Jiao, X.; Guo, W.; Hamoud, Y.A. Comparison of five Boosting-based models for estimating daily reference evapotranspiration with limited meteorological variables. PLoS ONE 2020, 15, e0235324.

[94] J. Friedman, T. Hastie and R. Tibshirani, Additive Logistic Regression: A Statistical View of Boosting. The Annals of Statistics, 28(2):337–407, 2000.

[95] Wright S. 1921. Correlation and causation. Journal of Agricultural Research XX(7):557–585.

[96] Chicco, D., Warrens, M. J., & Jurman, G. (2021). The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation. PeerJ Computer Science, 7, e623.

[97] De Myttenaere A, Golden B, Le Grand B, Rossi F. 2016. Mean absolute percentage error for regression models. Neurocomputing 192(1):38–48 DOI 10.1016/j.neucom.2015.12.114.

[98] Armstrong JS, Collopy F. 1992. Error measures for generalizing about forecasting methods: empirical comparisons. International Journal of Forecasting 08:69–80.

[99] Santra, A. ve Christy, C., 2012, Genetic Algorithm And Confusion Matrix For Document Clustering, International Journal of Computer Science Issues, 9(1).

[100] W.W. Cohen, R.E. Schapire, and Y. Singer, "Learning to Order Things," J. Artificial Intelligence Research, vol. 10, pp. 243-270, 1999.

[101] Huang, J., & Ling, C. X. (2005). Using AUC and accuracy in evaluating learning algorithms. IEEE Transactions on knowledge and Data Engineering, 17(3), 299-310.

[102] J. Egan, Signal Detection Theory and ROC Analysis. New York: Academic Press, 1975.

[103] D. Green and J. Swets, Signal Detection Theory and Psychophysics. New York: Wiley, 1966.

[104] C. Metz, "Basic Principles of ROC Analysis," Seminars in Nuclear Medcine, vol. 8, pp. 283-298, 1978.

[105] J. Swets, "Measuring the Accuracy of Diagnostic Systems," Science, vol. 240, pp. 1285-1293, 1988.

[106] K. Spackman, "Signal Detection Theory: Valuable Tools for Evaluating Inductive Learning," Proc. Sixth Int'l Workshop Machine Learning, pp. 160-163, 1989.

[107] F. Provost and T. Fawcett, "Analysis and Visualization of Classifier Performance: Comparison under Imprecise Class and Cost Distribution," Proc. Third Int'l Conf. Knowledge Discovery and Data Mining, pp. 43-48, 1997.

[108] F. Provost, T. Fawcett, and R. Kohavi, "The Case Against Accuracy Estimation for Comparing Induction Algorithms," Proc. 15th Int'l Conf. Machine Learning, pp. 445-453, 1998.

[109] B. Boser, I. Guyon, and V. Vapnik, "A Training Algorithm for Optimal Margin Classifiers," Proc. Fifth Conf. Computational Learning Theory, pp. 144-152, 1992.

[110] J.A. Hanley and B.J. McNeil, "The Meaning and Use of the Area under a Receiver Operating Characteristics (ROC) Curve," Radiology, vol. 143, pp. 29-36, 1982.

[111] Jonathon Klein D., Jeremy Sherrill B., Gabriella Morello M., TRNSYS 17: A transient system simulation program, solar energy laboratory, 2017.

[112] Elnour, M.; Meskin, N.; Khan, K.; Jain, R. HVAC system attack detection dataset. Data Brief 2021, 37, 107166.

[113] A. Qiu, Z. Yan, Q. Deng, J. Liu, L. Shang, J. Wu, Modeling of HVAC systems for fault diagnosis, IEEE Access 8 (2020), 146248–146262.

[114] Dubois, P. F.Python: batteries included. Comput. Sci. Eng.9, 7–9 (2007).

[115] Millman, K. J. & Aivazis, M.Python for scientists and engineers. Comput. Sci. Eng. 13, 9–12 (2011).

[116] Pedregosa F, Varoquaux G, Gramfort A, Michel V, Thirion B, Grisel O, Blondel M, Prettenhofer P, Weiss R, Dubourg V, et al. Scikit-learn: machine learning in python. J Mach Learn Res. 2011; 12:2825–30.

[117] Zito T, Wilbert N, Wiskott L, Berkes P (2008) Modular toolkit for data processing (mdp): a python data processing framework. Front Neuroinform 2(8):8.

[118] T. Schaul, J. Bayer, D. Wierstra, Y. Sun, M. Felder, F. Sehnke, T. Rückstieß, J. Schmidhuber, PyBrain, Journal of Machine Learning Research 11 (2010) 743-746.

[119] Hanke M, Halchenko YO, Sederberg PB, Hanson SJ, Haxby JV, Pollmann S (2009) PyMVPA: a python toolbox for multivariate pattern analysis of fMRI data. Neuroinformatics 7:37–53.

[120] C. Chih-Chung, L. Chih-Jen, Libsvm: A library for support vector machines, ACM Trans. Intell. Syst. Technol. 2 (3) (2011) 1–27.

[121] Fan, R.E.; Chang, K.W.; Hsieh, C.J.; Wang, X.R.; Lin, C.J. LIBLINEAR: A library for large linear classification. J. Mach. Learn. Res. 2008, 9, 1871–1874.

[122] Van Der Walt, S.; Colbert, S. C.; Varoquaux, G. The NumPy array: a structure for efficient numerical computation. Comput. Sci. Eng. 2011, 13, 22.

EKLER

EK A. Model ve Veri Parametreleri

Tablo A.1. XGBoost parametreleri.

Parametre		**Açıklama**
eta	:	Öğrenme oranıdır.
min_child_weight	:	Bir yaprak gerekli olan tüm gözlemlerin ağırlıklarının minimum toplamını ifade eder.
max_depth	:	Ağacın maksimum derinliğini ifade eder.
gamma	:	Bir ayırma yapmak için gereken minimum kayıp azaltmayı belirtir.
max_delta_step	:	Her yaprak çıkışı olup olmayacağının izin kontrolünü sağlar.
subsample	:	Verisetindeki örneklerin(sample,observation) her bir karar ağacında hangi yüzde ile kullanılacağını temsil eder.
colsample_bytree	:	Verisetindeki özelliklerin (feature) her bir karar ağacında hangi yüzde ile kullanılacağını temsil eder.
colsample_bylevel	:	Her seviye için sütunların alt örnek oranıdır.
lambda	:	L2 ağırlıklarda düzenleme terimidir. Bu değerin arttırılması modeli daha ölçülü hale getirir.
alpha	:	L1ağırlıklarda düzenleme terimidir. Bu değerin arttırılması modeli daha ölçülü hale getirir.
scale_pos_weight	:	Dengesiz sınıflar için yararlı olan pozitif ve negatif ağırlıkların dengesini kontrol eder.

EK A2: LightGBM model parametrelerinin açıklamaları

Tablo A.2. LightGBM parametreleri.

Parametre		**Açıklama**
num_leaves	:	Ağaç başına düşen yaprak sayısı
learning_rate	:	İterasyon hızı kontrolü
max_depth	:	Ağacın maksimum derinliğini
min_data	:	Bir yaprağın sahip olabileceği minimum veri sayısı
feature_fraction	:	Ağaç oluşturmak için her yinelemede rastgele seçilen özelliklerin oranı
bagging_fraction	:	Her yineleme için kullanılacak veri oranını belirtir ve genellikle eğitimi hızlandırmak için kullanılır.

EK A3: Veri kümesinde kullanılan kısaltmaların listesi

Tablo A.3. Veri kümesinde kullanılan kısaltmaların listesi.

Semboller	Açıklama	Alt Simge	Açıklama
T	Sıcaklık	z	Alan
U	Kontrol sinyali	ao	Çıkış havası
PMV	Tahmini ortalama oy	wo	Çıkış suyu
P	Güç	amb	Ortam
t	Zaman	y	Yıl
		d	Gün

EK A4: Veri parametrelerinin açıklaması

Tablo A.4. Veri parametrelerinin açıklaması.

Index	Sembol	Açıklama
1	t y	Yılın saati
2	t d	Günün saati
3	T amb	Ortam sıcaklığı (°C)
4-15	T zA 1-T zA 4,T zB 1-T zB 4,T zC 1 - T zC 4	Bölgelerin sıcaklığı (°C)
16-18	T aoA , T aoB , T aoC	Klima Santrali (AHU) besleme havasının sıcaklığı (°C)
19-21	T woA , T woB , T woC	Soğutma bataryası dönüş suyu sıcaklığı (°C)
22	T t	Soğutulmuş su deposunun sıcaklığı (°C)
23	T chiller	Chiller çıkış suyu sıcaklığı (°C)
24-36	U 1 - U 13	Kontrol sinyalleri
37-51	-	Sıcaklık ayar noktaları (°C)
52-63	PMV 1 - PMV 12	Bölgelerin termal konfor endeksleri
64	P total	HVAC sisteminin genel tahmini güç kullanımı (kJ/h)
65	label	Sistem durumunun etiketi

ÖZGEÇMİŞ

Ad-Soyad : Refik KİBAR

ÖĞRENİM DURUMU:

- **Lisans :** 2013, Sakarya Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Sistemleri Öğretmenliği
- **Lisans :** 2018, Sakarya Üniversitesi, Bilgisayar ve Bilişim Bilimleri Fakültesi, Bilgisayar Mühendisliği
- **Yükseklisans :** 2023, Sakarya Üniversitesi, Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı, Bilgisayar ve Bilişim Mühendisliği Programı

MESLEKİ DENEYİM VE ÖDÜLLER:

- Eylül 2015 – Temmuz 2019 yılları arasında Borsa İstanbul Recepbey Mesleki ve Teknik Anadolu Lisesi'nde Bilişim teknolojileri alanında öğretmen olarak çalıştı.
- Kasım 2020 – Eylül 2021 yılları arasında Borsa İstanbul Recepbey Mesleki ve Teknik Anadolu Lisesi'nde müdür yardımcısı olarak görev yaptı.
- Şubat 2022 tarihinden beri Borsa İstanbul Recepbey Mesleki ve Teknik Anadolu Lisesi'nde atölye şefi olarak görev yapmaktadır.
- Ocak 2022 ve Haziran 2022 tarihinde bakanlık tarafından, Temmuz 2022 tarihinde kaymakamlık tarafından başarı belgesi ile ödüllendirilmiştir.
- Aralık 2022 tarihinde kaymakamlık tarafından üstün başarı belgesi ile ödüllendirilmiştir.

TEZDEN TÜRETİLEN ESERLER:

DİĞER ESERLER: