T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YAZILIM TANIMLI AĞLAR VE NESNELERİN İNTERNETİ TEMELLİ AKILLI ŞEBEKELERDE ANOMALİ TESPİTİ

YÜKSEK LİSANS TEZİ

Hilal YILDIZ

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

AĞUSTOS 2023

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YAZILIM TANIMLI AĞLAR VE NESNELERİN İNTERNETİ TEMELLİ AKILLI ŞEBEKELERDE ANOMALİ TESPİTİ

YÜKSEK LİSANS TEZİ

Hilal YILDIZ

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Musa BALTA

AĞUSTOS 2023

Hilal YILDIZ tarafından hazırlanan "YAZILIM TANIMLI AĞLAR VE NESNELERİN İNTERNETİ TEMELLİ AKILLI ŞEBEKELERDE ANOMALİ TESPİTİ" adlı tez çalışması 09.08.2023 tarihinde aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı **Siber Güvenlik** Bilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı :	**Dr. Öğr. Üyesi Murat İSKEFİYELİ** Sakarya Üniversitesi	.....
Jüri Üyesi :	**Dr. Öğr. Üyesi Musa BALTA** (Danışman) Sakarya Üniversitesi	.....
Jüri Üyesi :	**Doç. Dr. Süleyman EKEN** Kocaeli 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 "YAZILIM TANIMLI AĞLAR VE NESNELERİN İNTERNETİ TEMELLİ AKILLI ŞEBEKELERDE 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.

(……/……/2023).

(imza)

Hilal YILDIZ

TEŞEKKÜR

Yüksek lisans eğitimim ve bu tez çalışmasının yürütülmesi sırasında bilgi birikimini ve desteklerini esirgemeyen çok değerli danışman hocam sayın Dr. Öğr. Üyesi Musa Balta'ya, çalışmamdaki makine öğrenmesi alanında yardıma ihtiyaç duyduğum her anda sorularımı cevaplayan ve yanımda olan kıymetli hocam sayın Dr. Öğr. Üyesi Deniz Balta'ya teşekkürlerimi sunarım.

Tez sürecimde zorlandığım ve motivasyonumu kaybettiğim anlarda destekleriyle beni canlı tutan arkadaşlarıma, elinden gelen her konuda yardımıma koşan canım kardeşim Mehmet Kaan Yıldız'a, bu süreci yakından takip ederek bana destek olan babam Şuayip Yıldız'a ve her zaman yanımda hissettiğim geniş aileme teşekkür ederim.

Son olarak, hayatımın her evresinde bana destek olarak bu günlere gelmemi sağlayan, beni bugünkü ben yapan çok değerli biricik annem Ayşe Yıldız'a, hayatım boyunca verdiği emeklerine, sonsuz sabrına ve her zaman doğru yolda ilerlemem için gösterdiği desteğine minnet ve teşekkürlerimi sunarım.

Ayrıca bu tez çalışmasını maddi olarak destekleyen Sakarya Üniversitesi Bilimsel Araştırma Projeleri (BAP) Komisyon Başkanlığına (Proje No: 2022-6-23-68) teşekkür ederim.

Hilal YILDIZ

İÇİNDEKİLER

Sayfa

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ v
TEŞEKKÜR..... vii
İÇİNDEKİLER..... ix
KISALTMALAR..... xi
TABLO LİSTESİ xiii
ŞEKİL LİSTESİ xv
ÖZET..... xvii
SUMMARY..... xix
1. GİRİŞ..... 1
1.1. Motivasyon ve Problemin Tanımlanması..... 1
1.2. Çalışmanın Amacı ve Geliştirilen Çözüm Yöntemi..... 5
1.3. Tez Organizasyonu..... 7
2. TEMEL BİLGİLER VE LİTERATÜR ARAŞTIRMASI..... 9
2.1. Akıllı Şebekeler..... 9
2.1.1. Akıllı şebeke mimarileri..... 13
2.1.1.1. NIST akıllı şebeke kavramsal modeli 13
2.1.1.2. SGAM (Smart grid architecture model)..... 14
2.2. Yazılım Tanımlı Ağlar 15
2.2.1. Yazılım tanımlı ağ mimari yapısı..... 21
2.3. Yazılım Tanımlı Akıllı Şebekeler 22
2.3.1. Örnek bir yazılım tanımlı akıllı şebeke mimari yapısı..... 28
2.4. IoT Temelli Akıllı Evler..... 28
2.4.1. Örnek bir IoT temelli akıllı ev mimari yapısı 35
3. YAZILIM TANIMLI AĞLAR VE NESNELERİN İNTERNETİ TEMELLİ BİR AKILLI EV AĞI MİMARİ ÖNERİSİ..... 37
3.1. Mimari Genel Bilgi..... 38
3.2. Modelleme ve Test Ortamı..... 40
3.2.1. SDN altyapısının oluşturulması 40
3.2.2. IoT altyapısının oluşturulması..... 43
3.2.2.1. Kullanılan cihazlar 44
3.2.2.2. Kullanılan protokoller 47
3.3. Senaryoların ve Veri Setlerinin Oluşturulması..... 50
3.3.1. Normal durumlardaki ev senaryolarının oluşturulması..... 50
3.3.2. Veri setlerinin oluşturulması 51
3.3.2.1. Normal durumlardaki veri seti 52
3.3.2.2. Saldırı durumlarındaki veri seti..... 52
4. MAKİNE ÖĞRENME ALGORİTMALARIYLA PERFORMANS ANALİZİ 55
4.1. Veri Ön İşleme 55
4.1.1. Veri temizleme..... 55
4.1.2. Veri azaltma 56

4.1.3. Veri ölçeklendirme 57
4.1.4. Veri bölümlendirme 58
4.2. Kullanılan Makine Öğrenme Algoritmalarının Performans Analizi 63
4.2.1. Performans analizi için kullanılan metrikler 64
4.2.2. Kullanılan makine öğrenme algoritmaları 65
4.2.2.1. En yakın komşu 65
4.2.2.2. Destek vektör makineleri 67
4.2.2.3. Karar ağaçları 68
4.2.2.4. Rastgele orman 69
4.2.2.5. Naïve bayes 70
4.2.2.6. Yapay sinir ağları 71
4.3. Algoritmaların Karşılaştırmalı Performans Analizi 73
5. TARTIŞMA VE SONUÇ 75
5.1. Sonuçlar 75
5.2. Çalışmanın Bilime Katkısı 76
5.3. İleriki Çalışmalar 77
KAYNAKLAR 79
EKLER 89
ÖZGEÇMİŞ 95

KISALTMALAR

AMI : Advanced Metering Infrastructure
API : Application Programming Interface
BTU : British Thermal Unit
CSGEC-23 : Center Smart Grid Energy Consumption-2023
DoS : Denial of Service
EPDK : Enerji Piyasası Düzenleme Kurumu
FN : False Negative
FP : False Positive
G2V : Grid to Vehicle
H2M : Human to Machine
HAN : Home Area Network
HEM : Home Energy Management
IAN : Industrial Area Network
IoT : Internet of Things
IP : Internet Protocol
IT : Information Technology
KNN : K-Nearest Neighbours
M2M : Machine to Machine
MITM : Man in the Middle
MQTT : Message Queuing Telemetry Transport
NERC : North American Electric Reliability Corporation
NIST : National Institute of Standards and Technology
OT : Operational Technology
PEVs : Plug-in Electric Vehicles
PLC : Programmable Logic Controller
SCADA : Supervisory Control and Data Acquisition
SDN : Software Defined Networking
SGAM : Smart Grid Architecture Model
SVM : Support Vector Machine
TCP : Transmission Control Protocol

TN : True Negative

TP : True Positive

V2G : Vehicle to Grid

WLAN : Wireless Local Area Network

WSN : Wireless Sensor Network

TABLO LİSTESİ

Sayfa

Tablo 2.1. Literatürdeki akıllı şebekeler ile ilgili çalışmalar 11
Tablo 2.2. Literatürdeki SDN ile ilgili çalışmalar 19
Tablo 2.3. Literatürdeki yazılım tanımlı akıllı şebekeler ile ilgili çalışmalar 26
Tablo 2.4. Literatürdeki IoT temelli akıllı evler ile ilgili çalışmalar 33
Tablo 4.1. Literatürdeki veri setlerinin karşılaştırması 60
Tablo 4.2. Karışıklık matrisi 65
Tablo 4.3. En yakın komşu algoritması için test sonuçları 67
Tablo 4.4. Destek vektör makinesi algoritması için test sonuçları 68
Tablo 4.5. Karar ağaçları algoritması için test sonuçları 69
Tablo 4.6. Rastgele orman algoritması için test sonuçları 70
Tablo 4.7. Naïve bayes algoritması için test sonuçları 71
Tablo 4.8. Yapay sinir ağları için test sonuçları 72

ŞEKİL LİSTESİ

Sayfa

Şekil 2.1. NIST akıllı şebeke mimarisi 13
Şekil 2.2. SGAM akıllı şebeke mimarisi 14
Şekil 2.3. Yazılım tanımlı ağ mimarisi 21
Şekil 2.4. Yazılım tanımlı akıllı şebeke mimarisi 28
Şekil 2.5. Akıllı ev mimarisi 35
Şekil 3.1. Önerilen yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı şebeke mimarisi 39
Şekil 3.2. Simülasyon ortamında oluşturulan akıllı ev topolojisi 41
Şekil 3.3. Önerilen akıllı ev mimarisi 44
Şekil 4.1. En yakın komşu algoritması modeli 66
Şekil 4.2. Destek vektör makinesi algoritması modeli 67
Şekil 4.3. Yapay sinir ağı modeli 71
Şekil 4.4. Algoritmaların performans karşılaştırması 74

YAZILIM TANIMLI AĞLAR VE NESNELERİN İNTERNETİ TEMELLİ AKILLI ŞEBEKELERDE ANOMALİ TESPİTİ

ÖZET

Günümüzde kullanılan geleneksel elektrik şebekelerinin sahip olduğu güvenilirlik sorunları, maliyet verimsizliği ve arz talep dengesinin sağlanamaması gibi olumsuzluklar yeni bir teknolojinin geliştirilmesine zemin hazırlamıştır. Son yıllarda adından sıkça söz ettiren akıllı şebekeler, esneklik, ölçeklenebilirlik, programlanabilirlik ve güvenilirlik gibi özellikleriyle bu ihtiyaca cevap verebilecek nitelikteki bir teknolojidir. Enerjinin üretim, iletim, dağıtım ve tüketim aşamalarında verim sağlarken sürdürülebilir enerji üretimini de destekler. Bunların yanı sıra, birçok cihazın ve protokolün bir arada çalıştığı heterojen ağ yapısı sebebiyle çeşitli zorlukları da beraberinde getirmektedir. Akıllı şebekelerdeki bu sorunların çözümü olarak önerilen SDN (Software Defined Networks, Yazılım tanımlı ağlar) ağ paradigması, merkezi yönetim sistemiyle ağ kaynaklarının kontrol edildiği bir teknolojidir. Cihazların performansını, izlenebilirliğini ve güvenliğini artırması sebebiyle SDN'nin akıllı şebeke ile entegrasyonu, enerji sektörünü daha verimli, güvenli ve sürdürülebilir bir hale getirirken aynı zamanda akıllı şebekelerin gelecekte daha yaygın kullanılması için önemli bir adımdır. Bunlarla beraber bu entegrasyon, enerji tüketicilerine, doğru faturalandırma ve tüketim analizi imkanı da tanır. Bunun ana sebeplerinden biri olan akıllı sayaçlar, akıllı şebekelerde tüketim alanındaki evlerde enerji üretim ve tüketim verilerinin anlık elde edilmesini sağlamaktadır. Günümüzde evlerde kullanımı oldukça yaygınlaşan IoT (Internet of Things, Nesnelerin interneti) destekli cihazların gelişmiş veri toplama ve işleme özellikleri, akıllı sayaçların sağladığı avantajlar ile birleştirildiğinde tüketicinin, evindeki enerji tüketimini anlık olarak izleyebildiği bir sistem haline gelir. Bu sistem, günümüzde oldukça yaygınlaşan akıllı ev sistemleridir.

Tüm bunlar ışığında bu tez çalışmasında, hem bahsi geçen teknolojilerin nasıl bir arada kullanılabileceğine dair bir bakış açısı sunmak hem de sonraki akademik çalışmalarda kullanılmak üzere gerçek enerji tüketim verilerini elde edebilmek amacıyla yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı ev mimarisi önerilmiştir. Önerilen bu mimari, günümüz akıllı ev sistemleri ve kullanıcıların beklentilerine göre tasarlanmış ve ardından Mininet isimli simülatörde gerçeklenmiştir. Akıllı evde bulunması planlanan 8 akıllı cihazın enerji tüketim bilgileri, detaylı literatür ve sektör araştırmaları sonucunda elde edilerek simülasyonunu sağlayacak kodlar geliştirilmiştir. Bu kapsamda simülatör çalıştırılarak bu tez çalışmasının bir diğer çıktısı olan enerji tüketim değerlerine ait veri seti oluşturulmuştur. Bu veriler, evdeki cihazlara karşı yaşanabilecek olası siber saldırıları da içerebileceğinden bunun tespiti için makine öğrenme algoritmaları kullanılarak enerji tüketiminin normal/anormal sınıflandırılması yapılmıştır. Kullanılan 6 farklı algoritmanın performans karşılaştırmasında rastgele orman modelinin en yüksek performansa sahip olduğu görülmüştür.

ANOMALY DETECTION IN SMART GRIDS BASED ON SOFTWARE-DEFINED NETWORKS AND THE INTERNET OF THINGS

SUMMARY

The problems such as reliability problems, cost inefficiency and supply-demand balance of the traditional electricity networks used today due to old technologies and one-way communication systems have paved the way for the development of a new technology. Smart grids, which have made a name for themselves in recent years, are a technology that can meet this need with their features such as flexibility, scalability, programmability and reliability.

It is possible to forecast energy demand and production, optimize energy resources and manage energy consumption thanks to the features of smart grids based on instant data collection, analysis and processing at every stage of energy generation, transmission, distribution and consumption. It is also important in terms of energy efficiency, as it prevents imbalances between energy demand and production, enabling more efficient use of energy resources. Thanks to real-time monitoring and management of energy consumption, it offers consumers the opportunity to consume energy at lower prices and real-time billing. In addition, the energy consumption habits of consumers are monitored, and suggestions are made to save energy.

Because of these advantages, smart grids are considered as an important part of the transformation process in the energy sector. However, some concerns such as energy security and privacy protection during the development and implementation of these systems are among the issues that are gaining more and more importance with the rapid spread of smart grids. In addition, due to the heterogeneous network structure in which many devices and protocols work together, it brings with it various difficulties. Examples of these challenges are managing integrated structures and solving problems.

SDN (Software defined networks) paradigm is suggested as a solution to such problems in smart networks. Based on the control of network resources with a central management system, this technology offers a different approach from traditional methods. In traditional network management, the control function is built into the network devices and the devices work in a structure that is connected to each other with fixed links. In other words, network components perform network management and control by communicating directly with each other thanks to the operating systems on them. On the other hand, in SDN technology, network management and control are performed by a central software controller, and connections between network components are created and managed on a software basis. The SDN structure is based on the separation of bus and control planes in the network. Network traffic is routed and managed in the bus plane, while centralized control of the network is provided in the control plane. Thanks to this working structure, the performance of the devices can be better managed, new services can be deployed more quickly, and the security of the network can be ensured more effectively.

The integration of SDN with the smart grid, as it increases the performance, traceability, and security of devices, is an important step for the future use of smart grids more widely, while making the energy sector more efficient, secure and sustainable. However, this integration plays an important role in how smart grids deal with heavy data traffic, thanks to the granularity feature of SDN. In addition, the heterogeneous structure of smart grids with different standards and protocols can achieve high performance with the management of the SDN controller. On the other hand, with this integration, energy consumers are provided with the opportunity of accurate billing and consumption analysis. Smart meters, which is one of the main reasons for this, provide instantaneous acquisition of energy production and consumption data in houses in the consumption domain of smart grids. These data obtained through smart meters can be collected and analyzed. In this way, it becomes possible for consumers to save money by monitoring their energy consumption habits.

IoT (Internet of Things) supported devices, which are widely used in homes today, are especially important in terms of collecting energy consumption data in a wider range. These devices can be white goods such as washing machines, refrigerators, dishwashers, as well as lighting, air conditioning systems or other sensor devices. IoT powered devices help transfer energy production/consumption and process data more accurately and reliably. This data then allows consumers to monitor and optimize their energy consumption in their homes. In addition, energy suppliers can use this data to manage their resources and become more efficient in terms of energy consumption. When these advanced data collection and processing features of IoT supported devices are combined with the advantages of smart meters, it becomes a system where the consumer can instantly monitor the energy consumption in their home. This system is called smart home systems, which are very common today.

Examples of IoT supported smart home systems are smart lighting, heating, security systems, air/water quality monitoring, smart lock systems and energy management systems. These automation systems aim to facilitate human life by personalizing the control of living spaces. Thanks to IoT devices, homeowners can control these systems remotely and make their daily lives easier. For example, monitoring energy use with a smart thermostat can optimize energy consumption by controlling the temperature in the home, which can also help homeowners save energy.

Monitoring and management of the smart home system is possible with the existence of a central management system. An example of this is the HEM (Home Energy Management) software. HEM software can be explained as a system in which energy consumption data is read from devices and managed according to user demands via the control panel. Devices in the smart home send their data here. Processes such as the analysis and processing of this data, the management of the house within the framework of certain rules and the storage of system data are carried out by HEM. Thanks to this software, users are given detailed information about the status and energy consumption of smart devices in their homes. Thus, the traceability of the smart home and the manageability of energy consumption are ensured.

All these technologies have some disadvantages as well as the advantages provided by their own working structures and integrations. For example, smart grids are vulnerable to cyber-attacks due to their heterogeneous structure that includes many different devices and protocols. Since the devices and energy consumption habits of consumers can be monitored in the smart grid architecture, it focuses on violating the private life of individuals. These data, collected for reasons such as increasing energy efficiency

and offering lower energy bills to consumers, constitute an important weakness in the protection of privacy. For this reason, it is necessary to take measures to protect private life in smart grids.

The use of SDN technology in smart networks also brings some security problems. The single point failure problem that SDN has due to its controls structure is a major security problem as it can make network systems vulnerable. While this issue can be circumvented by decentralizing SDN management using multiple controls, the newly exposed problem of a malicious node acting as controls is another challenge.

On the other hand, although the widespread use of IoT technologies provides great convenience in human life, it leads to security vulnerabilities and various risks if precautions are not taken. Privacy and security risks, risk of exposure to cyberattacks, data integrity issues, and network compatibility issues are among the risks that need attention. IoT devices form a network by connecting to each other over the internet, and the intervention of unauthorized persons in these networks may pose a security risk. In addition, the differences between these devices and the security of the different networks used also greatly affect IoT security.

These security issues are a major concern, especially when it comes to IoT-based smart homes. For example, cyber attackers can control the heating or cooling systems of the house. They can cause property damage by increasing their energy bills, or worse, they can cause a fire in the house by manipulating the heating system, causing loss of life and property. In addition, cyber attackers can also gain access to the personal data of the hosts. This data may include information about the host's movements, preferences, habits, location information, and even health.

As a result, the security of smart grids, SDN and IoT-based smart homes should be brought into focus and necessary precautions should be taken. Various security mechanisms can be used for this, such as network traffic monitoring, intrusion detection and prevention systems, firewalls, authentication and data traffic encryption.

In the light of all these, in this thesis, software-defined and IoT-based smart home architecture is proposed in order to both provide a perspective on how the mentioned technologies can be used together and to obtain real energy consumption data to be used in future academic studies.

In this architectural structure, the smart network structure proposed by NIST and consisting of 7 components (generation, transmission, distribution, consumption, market, service provider, management) was planned on the basis of SDN and the home area network within the consumption domain was designed as an IoT-based smart home system.

The proposed architecture in the study is modeled using a network virtualization tool called Mininet. In order to run the model in the simulation environment, the studies in the sector and the literature were examined in detail and the factors affecting the energy consumption and consumption values were determined for each smart device. In the light of the obtained parameters, a software has been developed that runs the model in the simulation environment in a realistic way. This software can imitate the energy consumed by the devices within the framework of the main features (energy class, volume, program, etc.) that affect the energy consumption.

In the second stage of the study, comprehensive working scenarios were determined by considering today's smart home structures and user profiles. System and consumption data were collected by running the scenarios in the simulator

environment. The data set, which is an output of the study, was created by arranging the generated data in an appropriate format. The data set was prepared by considering previous studies to contribute to the literature. In addition, a second data set including home attack scenarios was created to examine smart home systems within the framework of cyber security.

In the third stage of the study, the performance comparison of machine learning algorithms was made in the detection of anomalies in the created data sets. While choosing the algorithms to be used, attention was paid to the compatibility with the data set as well as the fact that it was preferred in other studies in the literature in terms of comparison. As a result, it has been concluded that the artificial neural network model has the best performance for anomaly detection in the smart home system energy consumption dataset.

1. GİRİŞ

1.1. Motivasyon ve Problemin Tanımlanması

Günümüzde kullanılan geleneksel elektrik şebekeleri, eski teknolojiler ve tek yönlü iletişim sistemleri nedeniyle giderek artan yetersizliklerle karşı karşıyadır. Bu yetersizlikler, güvenilirlik sorunları ve maliyet verimsizlikleri şeklinde kendini göstermektedir. Bunun sonucu olarak, yenilikçi akıllı şebeke teknolojilerinin benimsenmesi ve entegrasyonu hız kazanmaktadır. Akıllı şebekeler, enerji üretimi, iletimi, dağıtımı ve tüketimindeki her aşamada, gerçek zamanlı veri toplama, analiz etme ve işlemeye dayalı özellikleriyle, elektrik şebekelerinin verimli bir şekilde yönetilmesine olanak tanır.

Akıllı şebekeler sayesinde, tüm piyasa katılımcıları, enerji üreticileri, tüketiciler, enerji dağıtım şirketleri ve enerji depolama sistemleri birbirine bağlanarak verimli enerji tüketimini sağlar. Ayrıca, akıllı şebekelerin entegrasyonu, enerji üretiminin koordinasyonu ve izlenmesiyle enerji arzını yönetme imkanı sağlayarak enerji kaynaklarının daha verimli kullanımını ve sürdürülebilir enerji tedarik sistemlerinin oluşturulmasını sağlar. Bu nedenle, akıllı şebekeler, enerji sektöründe dönüşüm sürecinin önemli bir parçası olarak kabul edilmektedir.

Akıllı şebekeler, birçok farklı cihazın ve protokolün bir arada çalışmasını gerektiren karmaşık ve heterojen ağ yapısına sahiptir. Bu durum, tümleşik yapıların yönetilmesi ve sorunların çözülmesi konusunda zorluklar yaratabilmektedir. Bir cihazda yaşanan bir sorun, diğer cihazların ve hatta tüm sistemlerin performansını etkileyebilir. Diğer yandan akıllı şebekelerin güvenliği de önemli bir sorundur. Cihazların ve verilerin güvenliği konusunda sıkı güvenlik önlemleri alınması gerekmektedir.

Geleneksel ağlarda karşılaşılan esneklik, dinamik yönetim, programlanabilirlik, ölçeklenebilirlik ve güvenlik gibi sorunlar, günümüz akıllı şebekelerin mevcut ağ yapıları için de birer sorun olarak devam etmektedir. İncelenen akademik çalışmalar neticesinde akıllı şebekelerin ağ altyapıları için SDN ağ paradigmasının tercih edildiği gözlemlenmiştir [1-4].

Bu tercihin ana sebeplerinden biri SDN'in, şebeke cihazlarını ve ağ kaynaklarını, merkezi yönetim sistemiyle kontrol etmesidir. Bu sayede, cihazların performansı daha iyi yönetilebilmekte ve güvenliği artırılabilmektedir. SDN teknolojisi, veri ve kontrol düzlemlerinin ayrılması ilkesine dayanarak ağ yönetimini yeniden tanımlamaktadır. Veri düzleminde paketlerin yönetimi, kontrol düzleminde ise ağ trafiğinin genel yönetimi sağlanmaktadır. Bu sayede, ağ yöneticileri ağ trafiğini daha esnek bir şekilde yönetebilir, hızlı bir şekilde yeni hizmetleri devreye alabilir ve ağ güvenliğini daha etkili bir şekilde koruyabilirler. Böylece, enerji sektöründe daha verimli, daha güvenli ve daha sürdürülebilir bir enerji yönetim sistemi oluşturulması sağlanmaktadır. Tüm bu nedenlerle, SDN'nin akıllı şebeke ile entegrasyonu, akıllı şebekelerin gelecekte daha yaygın olarak kullanılması için önemli bir adım olarak kabul edilmektedir.

Diğer bir yandan akıllı şebeke sistemlerinin, enerji arz ve talebini doğru bir şekilde yönetebilmesi için tüketim domaini enerji üretim ve tüketim değerlerinin doğru ve net bir şekilde elde edilmesi ve merkeze taşınması gerekmektedir. Bu veriler, enerji üreticileri ve dağıtım şirketleri için doğru yatırım ve planlama kararları alınmasına yardımcı olur. Tüketiciler için ise, tüketim verilerinin doğru bir şekilde ölçülmesi, faturalandırmanın doğru yapılmasını sağlar.

Akıllı şebekelerde enerji üretim ve tüketim verileri, tüketim domaini içerisinde yer alan HAN (Home Area Network, Ev alan ağı) ve IAN (Industrial Area Network, Endüstri alan ağı) alanlarında kullanılan akıllı sayaçlar vasıtasıyla elde edilmektedir. Ev içi ağlarda bulunan akıllı sayaçlar, tüketicilerin evlerindeki enerji tüketimini anlık olarak takip etmelerine olanak tanır. Bu sayede, tüketicilerin enerji tüketim alışkanlıklarını analiz ederek tasarruf etmeleri mümkün hale gelir. Sanayi ağlarında (IAN) bulunan akıllı sayaçlar ise enerji yönetimini daha da etkili hale getirir. Sanayi üretiminde kullanılan makinelerin enerji tüketim verileri, akıllı sayaçlar aracılığıyla toplanarak analiz edilebilir hale gelir. Bu sayede, enerji tüketimindeki dalgalanmalar ve verimlilik sorunları tespit edilerek gerekli önlemler alınabilir.

HAN içindeki akıllı ev sistemlerinde bulunan IoT destekli cihazlar, enerji tüketim verilerinin daha geniş bir yelpazede toplanması bakımından özellikle önemlidir. Bu sistemler, evlerdeki farklı cihazların enerji tüketimini ölçerek verileri toplayabilir. Bu cihazlar, çamaşır makineleri, buzdolapları, bulaşık makineleri gibi beyaz eşyalar olabileceği gibi aydınlatma, iklimlendirme sistemleri veya diğer sensör cihazlarından oluşabilmektedir. IoT destekli cihazlar, enerji üretim/tüketim ve proses verilerinin

daha doğru ve güvenilir bir şekilde aktarılmasına yardımcı olur. Bu veriler, daha sonrasında tüketicilere evlerindeki enerji tüketimlerini izleme ve optimize etme imkanı sunar. Ayrıca, enerji tedarikçileri de bu verileri kullanarak kaynaklarını yönetebilir ve enerji tüketimi açısından daha verimli hale gelebilirler.

Akıllı şebekelerde tüketim verilerinin doğru bir şekilde ölçülmesi kadar bu verilerin doğru bir şekilde depolanması ve yönetilmesi de oldukça önemlidir. Bu nedenle, veri yönetimi ve analizi, akıllı şebekelerin vazgeçilmez bir parçasıdır. Verilerin bu sistemde kritik bir rol oynaması, veri güvenliğinin de hayati önem taşımasına neden olmuştur.

Güvenliğin en temel yapı taşlarından olduğu akıllı şebekeler, bünyesinde barındırdığı farklı cihazların sebep olduğu heterojen yapısından dolayı siber saldırılara açık bir haldedir. Bu cihaz çeşitliliğiyle birlikte akıllı şebekelerin HAN/IAN yapılarında çok farklı protokoller birlikte kullanılmaktadır. Hem bazı protokollerin kendi yapısında bulunan zafiyetler hem de protokol çeşitliliğinin fazla olması akıllı şebeke güvenliğini tehdit eden unsurlardır. Bu yapısı, akıllı şebekelerin geniş bir saldırı yüzeyine sahip olmasına sebep olmaktadır.

Akıllı şebekeler, saldırıların hedefi olabilecek birçok bileşen içermektedir. Saldırılar, akıllı sayaçları, HAN'ları, veri yönetim sistemlerini veya kontrol merkezlerini hedef alabilir. Örneğin, akıllı ev içindeki verilerin sayaçlara veya sayaçlardan merkeze iletimi sırasında kullanılan protokoller hedef alınarak verinin güvenliği tehdit edilebilir. Bazı protokollerin yapısında bulunan zafiyetler saldırganlar için bir fırsat olarak görülmektedir. Saldırgan, kullanılan protokolün zafiyetine uygun bir saldırı gerçekleştirerek verileri manipüle eder veya ele geçirerek kendi amaçları doğrultusunda kullanır. Bu durum, akıllı şebekenin genel güvenliğini tehdit ederken aynı zamanda kişisel verilerin güvenliğinin de ihlal edilmesi anlamına gelir. Diğer yandan, verilerin saklanması ve analizi sırasında da güvenlik ihlalleri olabilir. Örneğin, bir saldırgan verilerin depolandığı veri tabanına erişebilir. Bu durum, saldırganın tüm şebeke verilerine erişmesi anlamına gelir ve büyük bir facia ile sonuçlanabilecek durumlar yaşanabilir.

Son yıllarda dünya genelinde yaşanan siber saldırılar da bunu doğrular niteliktedir. Teknoloji çerçevesinde gelişen ve değişen dünyada görülmüştür ki, sistemlerin gelişim hızı artıkça ihtiyaç duyduğu güvenlik de aynı oranda artmaktadır. Çünkü bir sistemin

gelişmesi çeşitli kolaylıkları getirse de bununla birlikte saldırı yüzeyinin de artmasına sebep olur.

Artan saldırı yüzeyine karşı önlemlerin alınmaması, özellikle kritik altyapılar gibi sistemlerde insan hayatını doğrudan etkileyen sonuçlar doğurabilir. Kritik altyapılar, işleyişinde yaşanabilecek bir aksamanın kamu düzeninin bozulmasına, prestij kaybına, ülke çapında yaşanabilecek ekonomik hasara ve hatta can kaybına neden olabilecek sistemler olarak açıklanabilir. Bu sistemlere IT (Information Technology, Bilgi teknolojisi) alanından, telekomünikasyon, bankacılık, finans sistemleri örnek verilebileceği gibi OT (Operational Technology, Operasyonel Teknoloji) alanından, su, enerji ve ulaşım sistemleri örnek verilebilir [5].

Siber güvenliğin, kara, hava, deniz alanlarının yanında dördüncü saldırı alanı olarak eklenmesiyle birlikte ülkeler arasındaki rekabetin siber dünyada da yaşandığı görülmüştür. Son yıllarda kritik altyapılara yapılan saldırılar incelendiğinde birçoğunun özellikle enerji sistemleri üzerine yapıldığı gözlemlenmektedir. Bu saldırılardan en bilinenleri arasında Stuxnet ve Black Energy saldırıları örnek gösterilebilir.

Stuxnet, 2010 yılında İran nükleer faaliyetlerini sekteye uğratmak amacıyla kullanılan bir solucan yazılımdır. Bu solucan, Microsoft Windows işletim sistemine bulaşarak, kontrol sistemlerindeki Siemens PLC (Programmable Logic Controller, Programlanabilir Mantık Denetleyici) cihazlara zarar vermiştir. Saldırı sonucunda, İran'ın nükleer programındaki santrifüjler zarar görmüş ve nükleer materyal üretiminde büyük bir düşüş yaşanmıştır [6]. Bu saldırı sadece nükleer tesislere yönelik bir saldırı değil aynı zamanda endüstriyel kontrol sistemlerinin güvenliği açısından da önemli bir dönüm noktası olmuştur. Ayrıca bu saldırı, siber savaşların gerçek dünya sonuçlarına yol açabileceğini göstermesi açısından da önemlidir. Bir ülkenin diğer bir ülkenin nükleer programını sabotaj yoluyla etkisiz hale getirebileceğini ve bunun sonuçlarının da hayati tehlikelere yol açabileceğini göstermiştir.

Black Energy, 2015 yılında Ukrayna güç şebekesine yönelik yapılan bir saldırıdır. Saldırganlar, phising (oltalama) yöntemiyle şebeke çalışanlarının e-postalarını kullanmış ve şirket ağına dahil olmayı başarmıştır. Ardından, 30 trafo merkezinde elektriği kesen saldırganlar, Ukrayna'nın farklı bölgelerindeki yaklaşık 225.000 müşterinin altı saat kadar elektriksiz kalmasına sebep olmuştur. Siber güvenlik

alanında önemli bir kilometre taşı olan Black Energy saldırısı, gelecekte benzer saldırıların gerçekleşme riski nedeniyle sektörler arasında büyük bir farkındalık yaratmıştır [7].

Tüm bu yaşananlar da göstermektedir ki, siber güvenlik, genelde kritik altyapılar özelde ise akıllı şebekeler için kritik bir unsurdur. Siber güvenliğin temel prensibi olarak kabul edilen CIA kısaltması, Confidentiality (Gizlilik), Integrity (Bütünlük) ve Availability (Erişilebilirlik) kavramlarını ifade etmektedir. Siber güvenlik stratejilerinin oluşturulmasında kullanılan bu kavramlar sistemin veya sektörün ihtiyacına göre önceliklendirilebilir. Kritik altyapılardan en önemlileri arasında olan enerji sistemlerinin güvenlik stratejilerinde özellikle gizlilik ve bütünlük kavramları önemli bir rol oynamaktadır. Gizlilik, enerji şebekelerinde verinin güvenliği açısından oldukça önemlidir. Verinin gizliliği sağlanmadığı takdirde veri hırsızlığı, veri manipülasyonu ve benzeri siber saldırılar gerçekleşebilir. Bu durum, kullanıcıların kişisel bilgilerinin ifşa edilmesine ve şebeke güvenliğinin riske girmesine yol açabilir. Bütünlük kavramı ise verinin doğruluğunu ve bütünlüğünü korumayı amaçlar. Enerji şebekelerinde verinin doğruluğunun korunması, yanlış kararlar alınmamasını ve hatalı işlemlerin önüne geçilmesini sağlar. Veri manipülasyonu, bu prensibin ihlali anlamına gelir ve enerji şebekelerinde güç kaybı gibi çok ciddi sonuçlara yol açabilir. Bu sebeplerle, enerji şebeklerinde veri bütünlüğünü ve gizliliğini sağlayabilecek siber güvenlik önlemlerinin alınması zorunlu hale gelmiştir. Bu önlemler arasında, güvenli iletişim protokolleri kullanımı, saldırı tespit ve önleme sistemlerinin entegrasyonu, veri şifreleme, erişim kontrolleri, izleme ve güncellemelerin yapılması yer almaktadır.

Günümüz çalışmalarında SDN ve IoT ağ paradigmalarının akıllı şebekeler üzerinde uygulandığı görülmektedir. Bu tez çalışmasında, literatürde yapılan çalışmalardan farklı olarak HAN içerisinde bulunan SDN ve IoT mimarisi anlatılmıştır. Çeşitli IoT bileşenleri içeren mimari, normal ve saldırı durumlarında değerlendirilerek farklı senaryolar oluşturulmuş ve uygulanmıştır. Enerji tüketim değerlerindeki anormalliklerin tespiti için çeşitli makine öğrenme algoritmalarının performansı tartışılmıştır.

1.2. Çalışmanın Amacı ve Geliştirilen Çözüm Yöntemi

İncelenen akademik çalışmalar sonucunda bu tez çalışmasında, akıllı şebekelerde kullanılmak üzere SDN ve IoT mimari altyapısı birlikte önerilmiştir. Bu mimari yapı

ile oluşturulmuş simülasyon ortamında belirli akıllı ev senaryoları kapsamında üretilen veriler, normal ve saldırı durumunda yani anormal olarak değerlendirilerek özel bir veri seti oluşturulmuştur. Bu çalışmada oluşturulan veri seti üzerinde, akıllı şebekelerin HAN ağlarında geliştirilecek saldırıların tespitinde kullanılabilecek yöntemler hakkında bilgi sunması açısından, literatürde en çok kullanılan makine algoritmalarının performans analizleri yapılmıştır. Elde edilen sonuçlar bölüm 4'te açıklanmıştır. Yapılan çalışmanın bilimsel katkıları ise şöyle sıralanabilir:

1. İncelenen akademik çalışmalar neticesinde akıllı şebekelerin tüketim domaini içerisinde bulunan HAN'ların iletim ve uygulama altyapısı için önerilen SDN ve IoT teknolojilerinin entegre bir kullanımına rastlanılmamıştır. SDN teknolojisi, akıllı şebekelerin yönetimini ve kontrolünü merkezi bir noktadan sağlayarak, şebeke performansını artırırken güvenlik ve esneklik sağlayan bir çözüm sunar. Diğer yandan, veri toplanmasına ve analiz edilmesine olanak sağlayan IoT teknolojisi, akıllı şebekelerin etkin bir şekilde yönetilmesine ve optimize edilmesine yardımcı olur. Ayrıca SDN ve IoT teknolojilerinin birlikte kullanıldığı bir perspektiften bakıldığında cihazların ve sensörlerin entegrasyonunu kolaylaştıran SDN teknolojisi, akıllı evler için en önemli konulardan veri analizi ve siber güvenlik açısından önemli bir rol oynar. Tüm bu avantajlar sebebiyle bu tez çalışmasında, SDN ve IoT teknolojisinin birlikte kullanıldığı bir akıllı şebeke mimarisi önerilmiştir. Bu mimari, Mininet simülasyon ortamı kullanılarak gerçekleştirilmiş ve SDN altyapısına sahip küçük HAN alanları kurularak akıllı evleri temsil eden IoT temelli ağlar modellenmiştir. Bu modelde çalıştırılmak üzere geliştirilen Python kodları sayesinde, modellenen akıllı ev ağı gerçeğe yakın şekilde çalışan bir yapıdadır.
2. Akıllı şebekelerde en çok karşılaşılan güvenlik sorunlarından birisi olan enerji üretim/tüketim değerlerinin veri bütünlüğü ve gizliliği, literatürdeki birçok çalışmaya konu olmuştur. Bu çalışmalar incelendiğinde, enerji üretim/tüketim değerleri çerçevesinde yapılan analizlerin az sayıda senaryo altında ve dar bir kapsamda gerçekleştirildiği gözlemlenmiştir. Oysaki bir cihazın enerji tüketim değeri, sahip olduğu donanım, kullanım şekli ve kullanım sıklığı gibi birçok parametreye göre farklılık göstermektedir. Literatürdeki bazı çalışmaların bu parametreleri dikkate almamaları nedeniyle yetersiz veya hatalı sonuçlar ortaya koyduğu tespit edilmiştir. Bahsi geçen eksiklikten yola çıkılarak bu tez

çalışmasında, ileride yapılacak çalışmalara bir altyapı olması adına çok farklı ev senaryolarının hibrid bir şekilde uygulandığı kapsamlı ve özel bir veri seti olan CSGEC-23 (Center Smart Grid Energy Consumption 2023) oluşturulmuştur. Bu veri seti oluşturulurken mimaride kullanılan cihazların enerji tüketim değerleriyle birlikte bu tüketim değerlerini etkileyen fiziksel ve yazılımsal özellikleri de dikkate alınmıştır. Ayrıca, akıllı ev mimarisi modellenirken günümüz akıllı ev sistemlerine uygunluğu konusuna önem verilerek, veri setinin gerçeğe en yakın şekilde oluşturulması sağlanmıştır.

3. Akıllı şebekelerin güvenliği üzerine yayınlamış ulusal (Türkiye Cumhuriyeti Enerji ve Tabii Kaynaklar Bakanlığı, EPDK vb.) ve uluslararası standartlarda (NIST, NERC vb.) yer alan güvenlik kriterlerini de dikkate alarak geliştirilecek saldırı tespit sistemlerinde kullanılacak yöntemlere daha net karar verilmesine yardımcı olmak adına bu tez çalışmasında, literatürde anomali tespitinde en çok kullanılan makine öğrenme algoritmaları geliştirilen özel veri seti üzerinde çalıştırılarak performans karşılaştırılması yapılmıştır.

1.3. Tez Organizasyonu

Bu tez çalışması 5 ayrı bölümden oluşmaktadır. Bölüm 2'de akıllı şebekeler, SDN, yazılım tanımlı akıllı şebekeler ve IoT temelli akıllı evler konuları ayrı başlıklar altında incelenmiştir. Her bir başlıkta konu ile ilgili detaylı bilgi verilerek literatürdeki bazı çalışmalar incelenmiştir. Ardından, önerdiğimiz mimari yapıya ışık tutabilmesi açısından literatürdeki ilgili konuda oluşturulmuş mimari yapılar anlatılmıştır.

Bölüm 3'te bu tez çalışmasında önerilen yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı ev ağı mimarisi anlatılmıştır. Önce mimari hakkında genel bilgiler verilerek bu mimarinin oluşturulduğu modelleme ve test ortamından bahsedilmiştir. Önerilen mimarinin SDN ve IoT altyapıları anlatılarak kullanılan cihazlar ve protokoller detaylandırılmıştır. Simülasyon ortamında modellenen akıllı ev sisteminin çalışma senaryoları, normal ve saldırı durumları olmak üzere iki başlıkta incelenmiştir. Son olarak bu senaryoların simüle edilmesiyle, bu tez çalışmasının literatüre en büyük katkısı olan, elde edilen normal ve saldırı durumlarındaki veri setleri detaylı bir şekilde açıklanmıştır.

Bölüm 4'te ilk olarak bu tez çalışmasının çıktısı olan performans karşılaştırma işlemi için kullanılacak metrikler anlatılmıştır. Ardından, literatürde en çok kullanılan

makine öğrenme algoritmaları anlatılarak, oluşturulan veri setleri üzerinde kullanıldıklarında belirlenen metriklere göre performans sonuçları verilmiştir. Son olarak, algoritmaların veri seti üzerinde gösterdikleri performansların genel karşılaştırması yapılmıştır.

Tezin son bölümünde ise, akıllı şebekelerde kullanılmak üzere önerdiğimiz yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı ev ağı mimarisinin bir çıktısı olan veri setleri üzerinde çalıştırılan makine öğrenme algoritmalarının performans sonuçları, çalışmanın literatüre katkıları ve son olarak gelecekte yapılması planlanan çalışmalardan bahsedilmiştir.

2. TEMEL BİLGİLER VE LİTERATÜR ARAŞTIRMASI

2.1. Akıllı Şebekeler

Akıllı şebekeler, enerji üretimi, iletimi ve dağıtımının optimize edilmesini sağlayan bir teknolojik sistemdir. Enerji üretim ve tüketim verilerinin toplanması, işlenmesi ve analiz edilmesi için sensörler, iletişim altyapısı, veri analizi yazılımları ve yönetim sistemleri gibi ana bileşenlerden oluşmaktadır. Bu bileşenler sayesinde, enerji talebini ve üretimini tahmin etmek, enerji kaynaklarını optimize etmek ve enerji tüketimini yönetmek mümkündür [8].

Akıllı şebekeler, geleneksel elektrik şebekelerine kıyasla daha esnek, verimli ve etkin enerji yönetimi sağlaması sebebiyle enerji sektöründe büyük bir önem arz eden ve birçok avantajı da beraberinde getiren bir sistem haline gelmiştir.

Bu sistemler, yenilenebilir enerji kaynaklarının kullanımını arttırmak ve enerji tüketimindeki karbon salınımını azaltmak için enerji tüketimini optimize etmeyi amaçlamaktadır [9]. Ayrıca, enerji talebi ve üretimi arasındaki dengesizlikleri önleyerek enerji kaynaklarının daha etkin bir şekilde kullanılmasını sağladığından enerji verimliliği açısından da önemlidir. Enerji tüketiminin gerçek zamanlı olarak izlenmesi ve yönetilmesi sayesinde tüketicilere daha düşük fiyatlarla enerji tüketme imkanı sunmaktadır [10]. Ayrıca, tüketicilerin enerji tüketim alışkanlıkları da izlenerek, enerji tasarrufu sağlayacak öneriler sunulmaktadır. Dağıtık yenilenebilir enerji kaynaklarının daha fazla kullanımına olanak sağlaması sayesinde, yenilenebilir enerji kaynakları daha yaygın bir şekilde kullanılabilir hale gelmektedir. Bu nedenle, evlerde kurulacak güneş enerjisi panelleri sayesinde, evlerde üretilen enerji doğrudan şebekeye beslenebilmekte ve daha fazla yenilenebilir enerji kullanımı sağlanabilmektedir.

Bu nedenlerden dolayı, akıllı şebekeler gelecekte enerji tüketimi ve üretimi açısından önemli bir rol oynamaya devam edecektir. Ancak, bu sistemlerin geliştirilmesi ve uygulanması sırasında enerji güvenliği ve özel hayatın korunması gibi bazı endişeler, akıllı şebekelerin hızla yaygınlaşmasıyla birlikte giderek daha fazla önem kazanan konular arasında yer almaktadır.

Enerji güvenliği, enerjinin sağlanması, dağıtımı ve kullanımı sırasında herhangi bir aksaklık veya saldırı durumunda enerjinin sürekli ve güvenli bir şekilde kullanılabilmesini sağlama konusuna odaklanmaktadır. Akıllı şebekeler, birçok farklı cihaz ve sistem arasındaki etkileşimi artırdığından, bu tür saldırıların riski de artmaktadır. Bu nedenle, akıllı şebekelerin güvenliği, geleneksel şebekelere göre daha yüksek bir öncelik taşımaktadır. Özel hayatın korunması, tüketicilerin evindeki cihazlar ve enerji tüketim alışkanlıkları akıllı şebeke mimarisinde izlenebildiği için, kişilerin özel hayatının ihlal edilmesi konusuna odaklanmaktadır. Enerji verimliliğini artırmak ve tüketicilere daha düşük enerji faturaları sunmak gibi sebeplerle toplanan bu veriler, özel hayatın korunması konusunda önemli bir zafiyet teşkil etmektedir. Bu sebeple, akıllı şebekelerin özel hayatın korunması konusunda önlemler alması gerekmektedir.

Bu önlemlere, tüketicilerin verilerinin anonimleştirilmesi, sadece gerekli verilerin toplanması ve bu verilerin güvenli bir şekilde depolanarak kullanılması, olası siber saldırılara karşı şifreleme algoritmalarının kullanılması, güvenlik duvarları ve saldırı tespit/önleme sistemlerinin kullanılması gibi farklı yazılımsal ve donanımsal güvenlik çözümleri örnek verilebilir.

Sonuç olarak, akıllı şebekeler, enerji sektöründe önemli bir yere sahip olan ve birçok avantaj sağlayan sistemlerdir. Bu sistemlerin kullanımıyla birlikte, enerji verimliliği sağlanabilmekte, yenilenebilir enerji kaynaklarından elde edilen enerjinin kullanımı arttırılabilmekte ve enerji maliyetleri düşürülebilmektedir. Bu nedenle, akıllı şebekelerin geliştirilmesi ve kullanımının arttırılması, enerji sektörünün geleceği açısından önemlidir. Ancak, güvenlik ve gizlilik konuları da göz önünde bulundurulmalı, akıllı şebekelerin enerji güvenliği ve özel hayatın korunması konuları çözüme kavuşturulmalıdır. Güvenli akıllı şebekelerin daha yaygın ve verimli bir şekilde kullanılması amaçlanmalı ve enerji sektöründe yarattığı bu önemli dönüşümün sürdürülebilir, gizli ve özel hayata saygılı bir şekilde gerçekleşmesi sağlanmalıdır.

Akıllı şebekelerin önemi, enerji sektöründe yapılan araştırmalar ve uygulamalarla da desteklenmektedir. Bu alanda yapılan çalışmalar sayesinde, akıllı şebekelerin daha da geliştirilerek kullanıma hazır hale getirilmesi hedeflenmektedir. Özellikle, yapay zeka ve bulut bilişim teknolojilerinin akıllı şebekelerde kullanımı, sistemlerin daha verimli ve etkin hale gelmesine katkı sağlamaktadır. Son yıllarda akıllı şebekeler konusunda birçok araştırma yapılmıştır. Bunlardan bazıları Tablo 2.1.'de sunulmaktadır.

Tablo 2.1. Literatürdeki akıllı şebekeler ile ilgili çalışmalar [11-14].

Başlık	Yayın Yılı	Özet
A Critical Review of Edge and Fog Computing for Smart Grid Applications	2019	Bu makalede, artan cihaz sayısı, IoT ve toplanan verilerin miktarının akıllı şebekelerin karmaşıklığını artırdığı ve bulut bilişim mimarisinin artık etkili bir akıllı şebeke hizmeti sağlayamadığını belirtilir. Edge ve fog bilişiminin akıllı şebeke uygulamalarında kullanımının arttığı, ancak güvenlik, uyumluluk ve programlama modelleri gibi sorunları da açıklanır.
Internet of Things Applications as Energy Internet in Smart Grids and Smart Environments	2019	Bu makalede, IoT uygulamalarının akıllı şebekeler ve akıllı çevreler için nasıl etkinleştirildiği ve enerji interneti kavramının gelişimine nasıl katkıda bulunduğu incelenmiştir. Makale, enerji interneti kavramı ile ilgili gelecekteki araştırma fırsatları, zorluklar ve açık sorunlar hakkında bilgi vermektedir.
Energy meters evolution in smart grids: A review	2019	Bu makale, akıllı şebekelerde kullanılan akıllı sayaçların önemini anlatırken aynı zamanda akıllı şebekelerin kullanım zorluklarını tartışır. Çalışmanın devamında akıllı sayaçların, akıllı şebekelerin sunduğu zorluklara ne gibi çözümler sunabileceği ele alınmıştır.
A survey on smart grid technologies and applications	2020	Bu makalede, akıllı şebeke teknolojileri, ölçüm ve iletişim, bulut bilişim ve uygulamalar ayrıntılı olarak incelenmiştir. Bu çalışma, akıllı şebeke çalışan araştırmacılar ve mühendisler için önemli bir kaynak niteliğindedir. Akıllı şebekelere geçişte sistem işletmecilerine yardım etmeyi hedefler.

Tablo 2.1. (Devamı) Literatürdeki akıllı şebekeler ile ilgili çalışmalar [15-17].

Başlık	Yayın Yılı	Özet
Communication Technologies for Smart Grid: A Comprehensive Survey	2021	Bu makalede, akıllı şebekelerin iletişim teknolojileri, iletişim gereksinimleri, fiziksel katman teknolojileri, ağ mimarileri ve araştırma zorlukları hakkında kapsamlı bir araştırma sunulmaktadır.
Vulnerabilities and Strategies of Cybersecurity in Smart Grid-Evaluation and Review	2022	Bu çalışmada, akıllı şebeke bağlamında kapsamlı bir siber güvenlik araştırması sunulmaktadır. Siber güvenliği benimsemenin kontrol ve yönetim sistemleri üzerindeki etkisi tartışılmıştır. Ayrıca, makale, akıllı şebekedeki kontrol kararlarıyla ilişkili siber güvenlik konularını ve zorluklarını vurgulamaktadır.
A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning	2023	Bu makalede, akıllı şebekedeki DoS saldırılarının kapsamlı ve metodik bir tartışmasını sunarak, en yaygın saldırı vektörlerini ve bunların akıllı şebeke üzerindeki etkileri analiz edilmiştir. Ayrıca, akıllı şebekedeki DoS saldırılarına karşı algılama ve hafifletme teknikleri, mevcut yaklaşımların güçlü yönlerini ve sınırlamalarını içeren bir araştırma sunmaktadır.

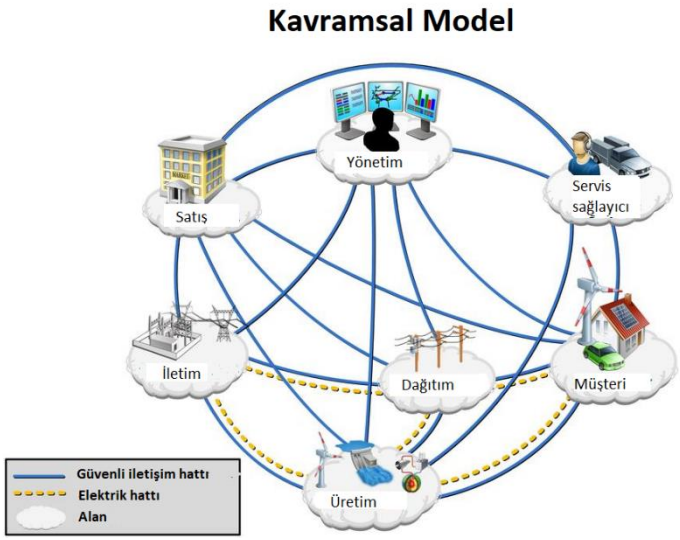
2.1.1. Akıllı şebeke mimarileri

Literatürde, akıllı şebeke bileşenlerinin işlevlerini ve birbirleriyle nasıl etkileşime girdiklerini farklı şekillerde tanımlayan mimariler mevcuttur. Bu mimarilerin ortak hedefi, enerji verimliliğini arttırmak, yenilenebilir enerji kaynaklarını entegre etmek, enerji güvenliğini sağlamak ve enerji tüketimi yönetimini kolaylaştırmaktır.

Çalışmanın bu bölümünde, literatürdeki akıllı şebeke mimarilerinden 2 tanesi incelenecektir.

2.1.1.1. NIST akıllı şebeke kavramsal modeli

NIST (National Institute of Standards and Technology, Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından geliştirilen ve ABD'deki akıllı şebeke uygulamalarının standartlaştırılması için tasarlanan mimari Şekil 2.1.'de gösterilmektedir.



Şekil 2.1. NIST akıllı şebeke mimarisi [18].

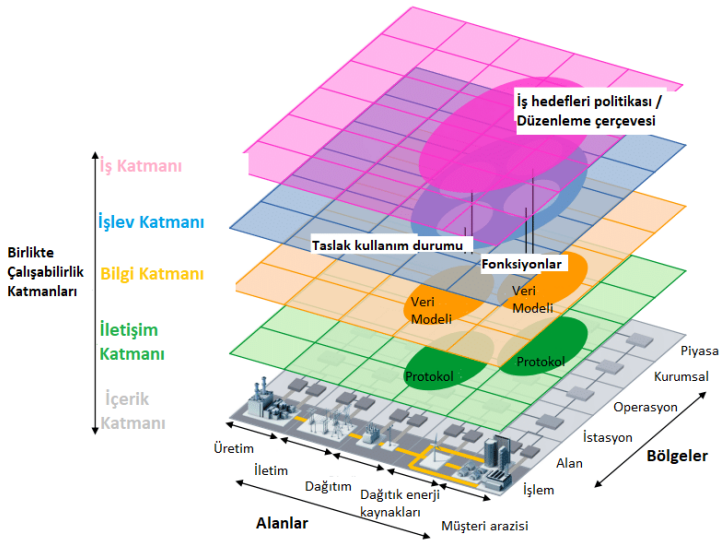
Bu mimari, şebeke bileşenlerini belirli işlevlere göre sınıflandıran ve her bir bileşen arasındaki iletişimi standartlaştıran bir çerçeve sunar [18]. Mimarideki şebeke bileşenler ve işlevleri şu şekilde özetlenebilir:

- Üretim: Enerjinin üretimini sağlayan alandır. Bu alanda, elektrik enerjisi üreten santraller, yenilenebilir enerji kaynakları gibi tesisler yer alır.
- İletim: Üretilen enerjinin dağıtım merkezlerine iletimi bu alanda yapılır. Bu alanda, yüksek gerilim hatları, iletim merkezleri gibi yapılar yer alır.

- Dağıtım: Enerjinin son kullanıcılara iletimi ve dağıtımı bu alanda yapılır. Bu alanda, şehirlerdeki sokak aydınlatmaları, evlere ve işletmelere enerji sağlayan dağıtım şebekeleri gibi yapılar yer alır.
- Müşteri/Tüketim: Enerji tüketen kişi veya kurumları temsil eder. Bu alanda, müşterilerin talepleri ve ihtiyaçları doğrultusunda enerji arz-talep dengesi sağlanır.
- Satış/Pazar: Enerjinin ticari faaliyetleri burada gerçekleşir. Bu alanda, enerjinin fiyatlandırılması, satışı ve dağıtımı gibi ticari işlemler yapılır.
- Hizmet Sağlayıcı: Enerji hizmetlerinin sağlayıcısıdır. Bu alanda, enerji tedarikçileri, dağıtım şirketleri ve enerji yönetimi hizmetleri sunan firmalar yer alır.
- Yönetim: Enerji üretim, iletim ve dağıtım sistemlerinin yönetimi bu alanda yapılır. Bu alanda, enerji üretim tesisleri, şebekelerin işletimi ve bakımı gibi faaliyetler gerçekleştirilir.

2.1.1.2. SGAM (Smart grid architecture model)

Avrupa Birliği tarafından geliştirilen mimari, akıllı şebeke bileşenlerini farklı katmanlara ayırarak tanımlar. Şekil 2.2.'de verilen bu katmanlar, fiziksel bileşenler, iletişim ağları, kontrol ve yönetim yazılımları ve iş uygulamalarıdır.



Şekil 2.2. SGAM akıllı şebeke mimarisi [19].

Mimaride akıllı şebekeler 5 ana bileşen kapsamında incelenmiştir [19]. Bu bileşenler ve işlevleri şöyledir:

- Toplu Üretim: Bu bölge, elektrik enerjisi üretim sistemlerini kapsar. Bu bileşenler, hidroelektrik santralleri, termik santraller ve nükleer santraller gibi kaynaklardan elektrik üretirler. Tipik olarak iletim sistemine bağlıdır.
- İletim: Elektrik enerjisinin üretim yerlerinden dağıtım şebekelerine ulaştırılmasından sorumlu alandır. Bu bölümde yüksek gerilim hatları ve transformatör istasyonları gibi büyük ölçekli ekipmanlar kullanılır. Bu alan, elektrik şebekesindeki büyük ölçekli güç iletimi ile ilgilidir.
- Dağıtım: Elektrik enerjisinin dağıtım şebekelerinden son kullanıcılara ulaştırılmasından sorumlu alandır. Bu bölümde orta gerilim hatları, dağıtım transformatörleri ve dağıtım panoları gibi ekipmanlar kullanılır. Bu alan, elektrik şebekesinin son aşamasındaki enerji iletimi ile ilgilidir.
- Dağıtık enerji kaynakları: Bu bölge, yenilenebilir enerji kaynakları gibi merkezi olmayan enerji üretim sistemleriyle ilgilidir. Güneş panelleri, rüzgar türbinleri ve mikro hidroelektrik sistemler gibi kaynaklar, tüketim bölgelerinde veya yakınında yerleştirilir ve elektrik enerjisi ağa dağıtılır.
- Müşteri arazisi: Bu bölge, tüketicilerin ev ve iş yerleri gibi yerlerinde kullanılan elektrikli cihazlar, aygıtlar ve ekipmanlar gibi enerji tüketimi ile ilgili bileşenleri kapsar. Bu bölge ayrıca, akıllı ev sistemleri, akıllı sayaçlar ve bina otomasyon sistemleri gibi diğer akıllı cihazlar için de bir arayüz sağlar.

2.2. Yazılım Tanımlı Ağlar

Günümüzde ağ teknolojilerinde hızlı bir gelişme yaşanmaktadır ve bu teknolojiler arasında en önemlilerinden biri yazılım tanımlı ağlar (SDN) olarak öne çıkmaktadır. SDN, ağ yönetimi ve kontrolü için yazılım tabanlı bir yaklaşım sunmaktadır ve geleneksel ağ yönetimi yöntemlerinden farklıdır.

Geleneksel ağ yönetimi, ağ cihazları (yönlendiriciler, anahtarlar vb.) üzerindeki kontrol işlevlerinin yerleşik olduğu ve cihazlar arasındaki bağlantıların sabit olduğu bir yapıda çalışır. Yani ağ bileşenleri birbirleriyle doğrudan iletişim kurarlar ve ağ yönetimi ve kontrolü, ağ cihazlarına yerleştirilen işletim sistemleri üzerinden gerçekleştirilir [20]. Ancak bu yapı, ağ yönetimindeki karmaşıklık arttıkça ölçeklenebilirlik ve yönetilebilirlik sorunları yaratabilir. Diğer yandan SDN teknolojisinde, ağ yönetimi ve kontrolü merkezi bir yazılım kontrolörü tarafından

gerçekleştirilir ve ağ bileşenleri arasındaki bağlantılar yazılım tabanlı olarak oluşturulur ve yönetilir. SDN yapısı, ağda veri yolu ve kontrol düzlemlerinin ayrıştırılması temeline dayanmaktadır. Veri yolu düzleminde ağ trafiği yönlendirilir ve yönetilirken, kontrol düzleminde ağın merkezi kontrolü sağlanır. Bu sayede, ağ yöneticileri, ağ trafiğini esnek bir şekilde yönetebilir, yeni hizmetleri daha hızlı bir şekilde devreye alabilir ve ağın güvenliğini daha etkili bir şekilde sağlayabilirler.

Günümüzde, SDN teknolojisi çeşitli alanlarda kullanılmaktadır. Özellikle bulut bilişim, veri merkezleri, IoT uygulamaları, büyük ölçekli şirket ağları, telekomünikasyon ve internet servis sağlayıcıları gibi ağın yoğun ve kompleks olduğu alanlarda SDN teknolojisi yaygın olarak kullanılmaktadır. Bu alanlarda, SDN, ağ yöneticilerine çeşitli avantajlar sunar. Bu avantajlar şu şekilde özetlenebilir:

- Merkezi Kontrol: Geleneksel ağlarda, ağ yöneticileri, her bir ağ cihazı için ayrı ayrı yapılandırma yapmak zorunda kalırlar. Bu, ağın büyüklüğüne bağlı olarak çok zorlu bir görev haline gelebilir. Ancak, SDN'de ağın merkezi kontrolünün yazılım tarafından sağlanması sayesinde, ağ yöneticileri ağın bütünündeki yapılandırmaları merkezi bir konumdan yönetebilirler. Bu sayede, ağın ölçeklenebilirliği artar ve ağ yönetimi daha kolay ve verimli hale gelir.
- Esneklik: Geleneksel ağlarda, ağ bileşenleri arasındaki bağlantıların sabit olması nedeniyle, ağa cihaz ekleme/çıkarma/değiştirme gibi değişiklikleri yapmak zordur ve genellikle manuel işlemler gerektirir [20]. Ancak, SDN yapısında bulunan kontrolör, ağda yeni hizmetlerin daha hızlı bir şekilde devreye alınmasına ve daha hızlı bir şekilde özelleştirilmesine olanak sağlar. Bu sayede, ağın uyarlanabilirliği artar ve özelleştirilmiş hizmetlerin kullanılması daha kolay hale gelir.
- Güvenlik: SDN, ağ güvenliğinin artırılması ve işlem yükü dağıtımının iyileştirilmesi gibi konularda avantajlar sağlar. Ağlardaki güvenlik açıklarının belirlenmesi ve ele alınması için SDN'nin esnek yapısı ve merkezi kontrol mekanizması kullanılabilir. SDN ayrıca, ağ güvenliği politikalarının merkezi bir şekilde uygulanmasını sağlayarak, ağdaki güvenlik açıklarının daha etkili bir şekilde tespit edilmesini ve ele alınmasını kolaylaştırır.
- Performans: SDN merkezi bir kontrol yapısına sahiptir. Bu, ağ yöneticilerinin ağın genel durumunu daha iyi anlamalarına ve ağ kaynaklarının kullanımını daha iyi optimize etmelerine olanak tanır. Ayrıca, ağın programlanabilir bir yapıya

sahip olması, ağ yöneticilerinin ağ kaynaklarını yazılım tabanlı bir yaklaşımla programlayarak, ağın işlevselliğini daha iyi kontrol edebilmesini sağlar. Böylece ağ kaynaklarının kullanımı daha etkili bir şekilde optimize edilir ve ağda verimlilik artar. Bu gibi sebeplerle, SDN ağın genel performansını artırmaktadır.

- Ekonomik Avantajlar: Geleneksel ağ yönetimi yöntemleri, her bir ağ bileşeni için ayrı bir işletim sistemine ihtiyaç duyar ve bu da daha fazla donanım ihtiyacı anlamına gelir. Ancak, SDN'de ağ yönetimi ve kontrolör yapısı sayesinde, ağ bileşenlerinde daha az donanım ihtiyacı vardır ve bu da ağ maliyetlerinin düşmesine yardımcı olur [21]. SDN, ağ kaynaklarının kullanımının optimize edilmesi, daha düşük maliyetler ve daha az enerji tüketimi gibi ekonomik avantajlar sağlar. Bu, ağ yönetiminde önemli bir etken olarak değerlendirilir.

Bu nedenlerle, araştırmacılar ve endüstri uzmanları SDN teknolojisinin daha fazla benimsenmesi ve yaygınlaştırılması için çalışmaktadırlar. Özellikle, SDN tabanlı ağ yönetim sistemlerinin geliştirilmesi ve SDN teknolojisine uygun yazılımların geliştirilmesi önemlidir. Bununla birlikte, SDN'nin geliştirilmesi ve iyileştirilmesi için standartlar belirlenmesi ve endüstri tarafından benimsenmesi önemlidir. Bu standartlar, SDN'nin farklı platformlar ve cihazlar arasında daha iyi bir şekilde çalışmasını sağlayacak ve SDN'nin yaygınlaştırılmasını hızlandıracaktır [22].

Tüm bunların yanında, SDN'nin bazı dezavantajları da vardır. SDN, yeni bir teknoloji olduğundan, ağ yöneticilerinin ve personelinin SDN ağlarını yönetmek için yeni beceriler edinmeleri gerekebilir. Bu, personel eğitimi ve öğrenme sürecinde ek çaba gerektirebilir. Ayrıca yeni bir teknoloji olmasından dolayı ağın donanım cihazlarının bu teknolojiyle uyumlu hale getirilmesi, yüksek maliyetli ekipmanlar satın alınması gerektirebileceğinden ekonomik yönde dezavantaj sağlar.

Merkezi kontrolör, SDN ağının doğru şekilde çalışması için sürekli olarak çalışır durumda olmalıdır. Bu, ağın merkezi kontrolörüne olan bağımlılığı artırır ve eğer kontrolör arızalanırsa, tüm ağın tamamen çökmesine neden olabilecek tek bir nokta hatası riskini taşır [23]. Bu risk siber saldırılar için de aynı şekilde değerlendirilebilir. Kontrol cihazı, ağ güvenliği için en kritik noktadır ve güvenlik açıklarına karşı daha fazla korunması gerekmektedir.

SDN, ağdaki trafiği yönlendirmek ve yönetmek için birçok yazılım bileşeni kullanır. Bu bileşenlerde güvenlik açıkları oluşabilir ve saldırganlar ağa sızarak aktif veya pasif

saldırılar gerçekleştirebilir. Pasif saldırı, saldırganın ağdaki trafiği izlemesi ile yapılan bir saldırı türüdür. Bu tür bir saldırıda, saldırgan pasif şekilde kalıp ağdaki trafiği dinleyebilir, veriler arasındaki hassas bilgileri ele geçirebilir veya ağdaki zayıf noktaları öğrenerek, daha sonra bu noktaları hedef alan aktif bir saldırı gerçekleştirebilir. Aktif saldırı, saldırganın ağa müdahale ederek ağda değişiklik yapması ile gerçekleştirilen, genellikle çok daha tehlikeli olan saldırı türüdür. Bu tür bir saldırıda, saldırgan ağ bileşenlerini veya sistemleri hedef alarak doğrudan müdahale edebilir. Örneğin ağa yanlış veri enjekte edebilir ve/veya veriyi yanlış yönlendirerek veri trafiğini manipüle edebilir veya ağda DoS (Denial of Service, Servis hizmet reddi) gibi saldırılar gerçekleştirebilir [24].

Bu risklerin azaltılması için çeşitli önlemler alınmalıdır. SDN, ağ kaynaklarına yüksek düzeyde erişim sağlar. Bu nedenle ağ yöneticileri, ağa erişimi olan herkesin yetkilerinin doğru bir şekilde yapılandırıldığından emin olmalıdır. SDN uygulamaları geliştirilirken siber güvenlik odak nokta haline getirilmeli ve uygulamaların ağ kaynaklarına erişim kontrolleri sıkılaştırılmalıdır. Bunun için, ağ trafiği izleme, saldırı tespit ve önleme sistemleri, güvenlik duvarları, kimlik doğrulama ve veri trafiği şifreleme gibi çeşitli güvenlik mekanizmaları kullanılabilir. Bahsedilen bu önlemler, SDN ağlarında güvenliği artırmak için alınabilecek önlemlerden sadece birkaçıdır. Bu öneriler, güvenlik politikaları çerçevesinde daha da geliştirilebilir [25].

Gelecekte SDN teknolojisinin sanallaştırma ve büyük veri gibi diğer teknolojilerle birlikte kullanılarak çok daha yaygınlaşacağı öngörülmektedir. Bu nedenle, SDN teknolojisinin geliştirilmesi ve iyileştirilmesi, ağ yönetimi ve güvenliği açısından önemli bir faktör olarak kalacaktır [22]. SDN'nin kullanımının artması beklenirken, SDN tabanlı ağ yönetim sistemlerinin geliştirilmesi ve SDN teknolojisine uygun yazılımların geliştirilmesi de önemlidir. SDN teknolojisi ile ilgili araştırmaların devam etmesi ve endüstri tarafından daha fazla benimsenmesi gerekmektedir.

Son yıllarda yazılım tanımlı ağlar konusunda birçok araştırma yapılmıştır. Bunlardan bazıları Tablo 2.2.'de sunulmaktadır.

Tablo 2.2. Literatürdeki SDN ile ilgili çalışmalar [26-28].

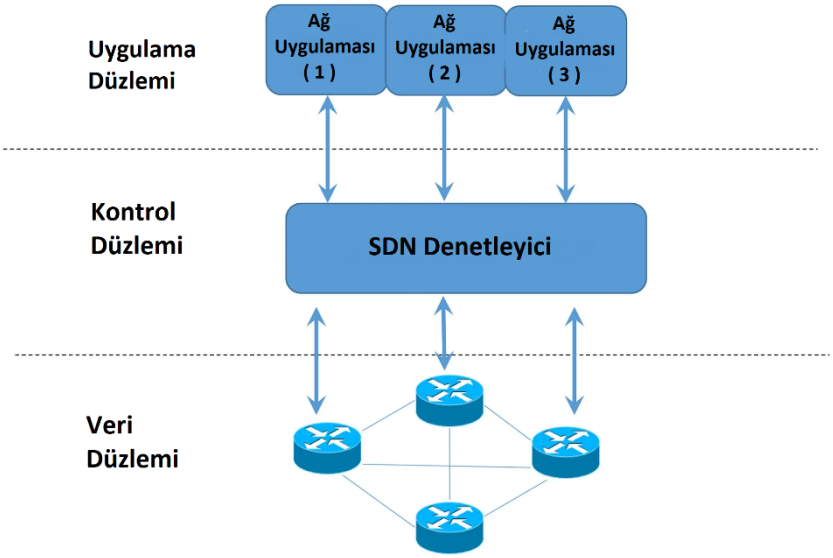
Başlık	Yayın Yılı	Özet
Software Defined Networking Architecture, Security and Energy Efficiency: A Survey	2017	Bu makalede, SDN tarafından çözülen çeşitli güvenlik tehditleri ve SDN uygulamasının ortaya çıkardığı yeni tehditler, enerji verimliliği ve ağ güvenliği konusundaki farklı stratejiler ve bu alanın geleceği tartışılmaktadır.
Controllers in SDN: A Review Report	2018	Bu makale, merkezi karar verme yeteneğiyle ağ performansını artıran SDN mimarisini inceleyen bir çalışmadır. Mevcut SDN kontrolörlerinin mimari genel bakışı, tasarım yönleri, verimlilik özellikleri vb. hakkında bilgi vermektedir. Ayrıca, endüstride ve akademide kullanılan başlıca popüler kontrolörleri ve bunların performansını ölçmek için kullanılan metrikleri ele almaktadır.
Complementing IoT Services Through Software Defined Networking and Edge Computing: A Comprehensive Survey	2020	Makale, SDN ve EC teknolojilerinin, IoT hizmetlerinin kalitesini ve güvenilirliğini artırmak için nasıl kullanılabileceğine dair kapsamlı bir literatür taramasını sunmaktadır. Ayrıca çalışma, SDN ve EC teknolojilerinin, IoT hizmetlerinin güvenilirliği ve kalitesinin artırılmasına yardımcı olabileceğini ve gelecekte bu teknolojilerin IoT hizmetlerinde daha yaygın olarak kullanılacağını öngörmektedir.

Tablo 2.1. (Devamı) Literatürdeki SDN ile ilgili çalışmalar [29-32].

Başlık	Yayın Yılı	Özet
Security in SDN: A comprehensive survey	2020	Bu makalede, SDN'yi tehdit eden güvenlik tehditlerinden bahsedilmiş ve mevcut literatür çalışmaları incelenmiştir. SDN-for-security ve SDN-security kavramları arasındaki farklar anlatılmıştır. SDN güvenliği alanındaki fırsatları ve gelecekteki zorlukları vurgulanmıştır.
Configuration and Governance of Dynamic Secure SDN	2021	Bu çalışmada, Dinamik ağlara çeviklik kazandırmak için SDN veri düzlemlerinin konfigürasyon ve yönetişiminden sorumlu ek bir düzlem ve bu düzlemi kullanan üç mimari önerilmiştir. Ardından, bu mimariler değerlendirilerek sonuçlar tartışılmıştır.
Software-Defined Networking: Categories, Analysis, and Future Directions	2022	Bu makale, SDN'deki birkaç mevcut yaklaşımı değerlendirmekte ve bulguları karşılaştırıp analiz etmektedir. SDN uygulamasıyla ilgili ağ güvenliği ve yönetim sorunları, bellek yönetimi çalışmaları, başta olmak üzere yedi kategoride değerlendirme yaparak her kategori için avantajlar ve dezavantajlar tartışılmıştır.
A Novel Dynamic Software-Defined Networking Approach to Neutralize Traffic Burst	2023	Bu çalışma, dinamik denetleyici eşleme algoritmalarının geliştirilmesi gerekliliği üzerinde duruyor. Böylece, denetleyicilerin trafik yüküne göre dinamik şekilde eşleştirilmesini sağlayarak ağ gecikmelerini azaltarak genel performansı artırmak amaçlanmıştır. Bu yaklaşımın, gecikme ve trafik dalgalanması sorunlarına etkili bir çözüm olduğu öngörülmektedir.

2.2.1. Yazılım tanımlı ağ mimari yapısı

Geleneksel ağ mimarisinden farklı olarak SDN mimarisinde, ağ donanım ve yazılım bileşenlerine ayrılmakta ve ağın kontrolü merkezi bir denetleyicide toplamaktadır. SDN'nin katmanlı mimari yapısı Şekil 2.3.'te gösterilmiştir.



Şekil 2.3. Yazılım tanımlı ağ mimarisi.

Veri, kontrol ve uygulama katmanlarından oluşan bu mimari yapıda, katmanlar arasındaki haberleşme açık kaynak protokoller/API'ler (Application Programming Interface, Uygulama programlama arayüzü) tarafından sağlanır [33].

- Veri düzlemi: Altyapı katmanı olarak da adlandırılan bu katman, router, switch gibi ağ cihazlarından oluşur. Görevi, ağ içindeki paketlerin ilgili kurallara göre iletimini sağlamaktır.
- Kontrol düzlemi: SDN işlevlerini denetleyen kontrolörünün bulunduğu katmandır. Veri katmanı ve uygulama katmanı arasında aracı görevi görür. Ağın genel durumunu izlemekten ve yönetimini sağlamaktan sorumludur. Ağ yöneticilerinin cihazların davranışlarını programlayarak sağlanan bu yönetim, yönlendirme, akış iletme ve paket bırakma işlevlerinden oluşur.
- Uygulama düzlemi: Ağ ve güvenlik uygulamalarının yürütüldüğü katmandır. IPS/IDS yazılımları, güvenlik duvarı uygulamaları, ağ sanallaştırma gibi uygulamalar bu katman tarafından yürütülür. Bu katmanda yürütülen uygulamalar sayesinde, ağ yöneticileri, ağdaki uygulamaların performansını izleyebilir ve uygulamaların ağa olan etkisini kontrol edebilirler [34].

SDN mimarisinde katmanlar arasındaki iletişim bağlantıları farklılık gösterir. Uygulama katmanı ve kontrol katmanı arasındaki iletişim, Northbound Communication (Kuzey yönlü iletişim) adı verilen bağlantı ile sağlanır. Uyulama katmanında çalışan uygulamalar, ağ hakkında bilgi almak veya ağ davranışının bir bölümünü veya tamamını yönetmek istediğinde Northbound Communication bağlantısıyla kontrol katmanında bulunan SDN kontrolörü ile iletişim kurar. Bu haberleşmenin sağlanabilmesi için REST API kullanılmaktadır [35].

Veri katmanı ve kontrol katmanı arasındaki iletişim ise Southbound Communication (Güney yönlü iletişim) bağlantısıyla sağlanır. SDN kontrolörü, veri katmanında bulunan cihazların yönetiminde bu bağlantıyı kullanır. Yönlendirme öğeleri buradan kontrol edildiğinden, bu bağlantının her zaman kullanılabilir ve güvenli kalması önemlidir. Haberleşmenin sağlanabilmesi için Openflow ve ForCES protokolleri kabul görmüştür.

2.3. Yazılım Tanımlı Akıllı Şebekeler

Gün geçtikçe artan enerji talebi sebebiyle elektik enerjisi sektöründeki koşullar değişmekte ve gelişmektedir. Hali hazırda kullanılan geleneksel güç şebekelerinin bu gelişime ayak uydurmakta zorlandığı görülmektedir [36]. Geleneksel güç şebekesinde, elektrik tipik olarak fosil yakıta dayalı elektrik üretim ünitelerinde (nükleer, hidro ve kömürle çalışan elektrik santralleri gibi) üretilir ve daha sonra geniş bir iletim hattı ağı aracılığıyla tüketicilere iletilir [37, 38]. Ek olarak, elektrik akımı tek yönlüdür, yani üretim birimlerinden tüketicilere doğrudur. Sürekli artan elektrik talebi, eski altyapı sorunları, güvenilirlik ve yenilenebilir enerji kaynaklarının önemi nedeniyle, geleneksel elektrik şebekesi artık uygulanabilir bir çözüm değildir. Bu sebeple, mevcut zorlukları etkin bir şekilde çözen bir yapı sağlamak amacıyla daha iyi bir teknoloji olan akıllı şebeke sistemlerine geçilmesi gerekmektedir.

Akıllı şebekeyi geleneksel elektrik güç şebekesinden ayıran temel özellikleri, iki yönlü iletişim yapabilme ve ağdaki kaynaklar üzerinde otomatik kontrol sağlama yeteneği ile talep yönetimi ve gerçek zamanlı fiyatlandırmadır. Bunu, ağdaki enerji gibi veri paketlerini de iletebilmesiyle yapar. Akıllı şebekedeki bu önemli gelişme, akıllı sayaç ve sensör cihazları kullanarak çift yönlü iletişimi mümkün kılan IoT ve WSN (Wireless Sensor Network, Kablosuz sensör ağlar) teknolojilerinin faydalarından yararlanılmasıyla gerçekleştirilmiştir [13, 39, 40].

Bu gelişmeyle birlikte, AMI (Advanced metering infrastructure, Gelişmiş sayaç altyapısı), PEVs (Plug-in electric vehicles, Tak-çalıştır elektrikli araçlar), SCADA sistemleri (Supervisory Control and Data Acquisition, Merkezi denetim ve veri toplama) ve yenilenebilir enerji kaynakları, akıllı şebekenin vazgeçilmez parçaları olacaktır.

Bugün birçok ülkede %100 yenilenebilir enerjiye dayalı geleceğe ulaşmak, ana hedeflerden biridir [41]. Bu bağlamda, yenilenebilir enerji kaynaklarının akıllı şebekeye entegrasyonu için literatürde önerilen birçok yol haritası mevcuttur. Akıllı evler, yenilenebilir enerji kaynaklarının büyük ölçüde kullanıldığı yerlerdir. Güneş panelleri gibi evde kullanılabilen yenilenebilir enerji kaynakları, önemli miktarda enerjiyi akıllı şebekeye geri verebilir [42]. Bu, akıllı sayaç kullanımıyla birlikte değerlendirildiğinde akıllı evlerdeki tüketicilerin, gerçek zamanlı fiyatlandırma ve faturalandırma beklentisinin karşılanması noktasında da önemli bir unsurdur.

Günümüz koşullarında birçok ihtiyaca cevap veren akıllı şebekelerin, yeniden yapılandırma gereken durumlarda hizmet kesintisine uğraması büyük bir dezavantajdır [43]. Bunun önüne geçmek için SDN teknolojisi önerilerek, yazılım tanımlı akıllı şebeke kavramı literatürde kendine önemli bir yer bulmuştur.

Akıllı şebekeler, enerji şebekelerindeki enerji üretim, dağıtım ve tüketimini gerçek zamanlı olarak izleyerek enerji akışını optimize eder. Bu işlevi sebebiyle, kontrolü sağlamak için iletişim ağlarına yoğun bir şekilde bağlıdır. Bu sebeple, akıllı şebeke sistemlerindeki iletişim varlıklarını yönetebilmek için SDN teknolojisinin uygulanması önerilmektedir. Böylelikle akıllı şebekelerde verimlilik ve dayanıklılık potansiyel olarak artırılabilir.

Yazılım tanımlı akıllı şebeke mimarisinin geliştirilmesi birçok avantajı da beraberinde getirmiştir. Örneğin, şebeke veri trafiği gecikmeye dayanıklı değildir ve megabaytlarca veri aktarımı gerektirebilir. Bu nedenle, kritik ölçüm verileri ve kontrol komutları zamanında iletilmeli ve normal trafikten daha yüksek önceliğe sahip olmalıdır. SDN denetleyicisi trafiği önceliklendirerek, AMI'den hizmet sağlayıcıya aktarırken iletim sayısını azaltarak verimliliği artırabilir. SDN'in ayrıntı düzeyi özelliği sayesinde gerçekleştirilen bu trafik akışı orkestrasyonu, akıllı şebekelerin yoğun veri trafiğiyle başa çıkmasında önemli bir rol oynar [44]. Ayrıca akıllı

şebekelerin farklı standartlar ve protokollere sahip heterojen yapısı, SDN kontrolörünün yönetimi ile yüksek başarıma ulaşmaktadır.

Yazılım tanımlı akıllı şebekelerde, coğrafi alan veya iletim, dağıtım ve güvenlik bölgeleri dikkate alınarak sanal ağ dilimleri oluşturulabilir. Böylelikle sanallaştırılan bölge, kendi ihtiyaçlarına yönelik güvenlik, yönetim ve servis politikalarına sahip olabilir. Bazen, bölge yerine belirli bir trafiğin izolasyonuna da ihtiyaç duyulabilir. SDN'in yetenekleri sayesinde farklı trafik türleri ve/veya uygulamaları şebeke ağında kolayca izole edilebilir [45].

Şebeke ağları söz konusu olduğunda bağlantının sürekliliği konusu büyük ölçüde önemlidir. Bu sebeple, akıllı şebekenin düzgün çalışması için bağlantı arızalarının tespit edilmesi ve önlenmesi gerekir. Fakat bazı durumlarda bu bağlantılar tıkanabilir veya bozulabilir. Yazılım tanımlı akıllı şebekelerde SDN'in hızlı bağlantı arızası tespit etme yeteneği sayesinde bu problemin önüne geçilebilmektedir. Bağlantı arızalarının yanında, elektrik şebekesi bazen aşırı yüklenebilir ve gerilim çökmesi meydana gelebilir. Bunun önüne geçmek için hat yükü dalgalanmalarının tespit edilip zamanında kaydırılarak gerilim çökmesinin önlenmesi gerekir. Bu, yazılım tanımlı ağlarda kolaylıkla sağlanabilmektedir [46].

Tüm bu avantajlarının yanında yazılım tanımlı akıllı şebekelerin de bazı dezavantajları vardır. Örneğin, şebeke sisteminde kullanılan ve SDN teknolojisine uyumlu olmayan cihazların değiştirilmesi ve bununla birlikte teknik personelin de bu yeni teknolojiye hazır hale getirilmesi gerekmektedir. Bu durum hem para hem de zaman maliyeti anlamına geldiğinden mevcut şebeke sisteminin yazılım tanımlı hale getirilmesi büyük topolojiler için pahalı ve mümkün olmayabilir. Ayrıca, SDN teknolojisinin akıllı şebekelerde kullanımı bazı güvenlik sorunlarını da beraberinde getirmektedir. SDN'in kontroller yapısından dolayı sahip olduğu tek nokta arızası problemi, şebeke sistemlerini savunmasız hale getirebileceğinden büyük bir güvenlik problemi teşkil eder. Birden fazla kontroller kullanarak SDN yönetimini merkezi olmayan bir hale getirerek bu sorunun önüne geçilebiliyor olsa da yeni durumda açığa çıkan, kötü niyetli bir düğümün kontroller gibi davranması problemi, aşılması gereken başka bir zorluktur [47-49].

Sonuç olarak, yazılım tanımlı akıllı şebekeler enerji sektöründe önemli bir teknolojik yenilik olarak karşımıza çıkmaktadır. Yazılım tanımlı akıllı şebeke teknolojisi, enerji

şebekelerinin daha verimli, daha sürdürülebilir, daha güvenli ve daha akıllı hale getirilmesine olanak sağlamaktadır. Ancak birçok teknolojide olduğu gibi bu teknolojinin de tam potansiyelinden yararlanılabilmesi için, birçok zorluğun üstesinden gelinmesi gerekmektedir. Bu nedenle, yazılım tanımlı akıllı şebeke teknolojisi üzerine daha fazla araştırma yapılması ve uygulamalarının yaygınlaştırılması için çalışmalar yapılması gerekmektedir.

Son yıllarda yazılım tanımlı akıllı şebekeler konusunda birçok araştırma yapılmıştır. Bunlardan bazıları aşağıdaki Tablo 2.3.'de sunulmuştur.

Tablo 2.3. Literatürdeki yazılım tanımlı akıllı şebekeler ile ilgili çalışmalar [50, 51, 1].

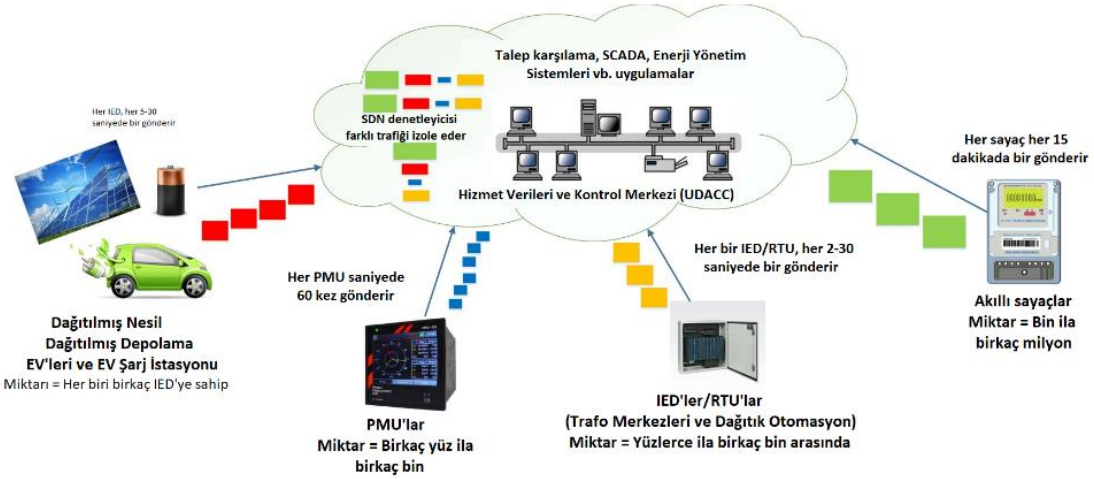
Başlık	Yayın Yılı	Özet
Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges	2015	Bu makalede, SDN kavramı ele alınmış ve SDN'nin akıllı şebekelerin direncini artırma potansiyeli, SDN'nin getirdiği riskler, bu risklerin yönetimi ve SDN tabanlı dayanıklılık çözümlerinin doğrulanması ve değerlendirilmesi konularında araştırmalar yapılmıştır. Makale, akıllı şebekeler için yenilikçi SDN tabanlı çözümlere ilham olmayı amaçlar.
Decentralized Cloud-SDN Architecture in Smart Grid: A Dynamic Pricing Model	2018	Bu çalışmada, elektrikli araçların şarj ve deşarj hizmetleri ve bina enerji yönetimi için gerçek zamanlı dinamik fiyatlandırma modeli önerilmiştir. Önerilen yaklaşım, SDN teknolojisi ve ağ işlevi sanallaştırma (NFV) temelli merkezi olmayan bir bulut bilişim mimarisi kullanır. Çalışmanın sonucunda, önerilen modelin şebeke yükünü optimize ettiği, elektrikli araç kullanımını artırdığı ve şebeke stabilitesini koruduğu gösterilmiştir.
Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey	2019	Bu çalışma, SDN temelli akıllı şebeke iletişiminin avantajları, örnek mimarileri, yönlendirme şemaları ile gizlilik ve güvenlik düzenlemelerini inceleyen kapsamlı bir araştırma sunmaktadır. Bu araştırma sonucunda, ileriye dönük zorluklar, açık sorunlar ve gelecek araştırma yönleri tartışılmaktadır.

Tablo 2.3. (Devamı) Literatürdeki yazılım tanımlı akıllı şebekeler ile ilgili çalışmalar [52-54].

Başlık	Yayın Yılı	Özet
Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency	2019	Makalede, SDN tabanlı bir IIoT platformu önerilmiştir. Platform, gerçek zamanlı izleme yaparak akıllı şebeke ağlarının başarısızlıklarına anında tepki verip kurtarılmasını sağlayacak şekilde tasarlanmıştır. Çalışmanın sonucunda, önerilen platformun akıllı şebeke dayanıklılığını artırabileceği gösterilmiştir.
A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System	2020	Makalede, IoT'ye dayalı bir sağlık sistemi için SDN tabanlı Edge bilişim mimarisi kullanarak güvenli bir çerçeve tasarlanmıştır. Çerçevede, IoT cihazları hafif bir kimlik doğrulama şeması kullanarak Edge sunucuları tarafından doğrulanmaktadır. Çalışmanın sonucunda, önerilen çerçevenin IoT'ye dayalı sağlık sistemleri için daha iyi çözümler sağladığını göstermektedir.
UCB-Based Route and Power Selection Optimization for SDN-Enabled Industrial IoT in Smart Grid	2022	Bu çalışmada, ağ yapılandırmasını basitleştirmek için yazılım tanımlı ağ tabanlı IIoT ağ çerçevesini benimseyen çok sekmeli iş birliği modu gelişimini desteklemek için üst güven sınırı (UCB) tabanlı ortak rota ve güç seçimi optimizasyon algoritması önerilmiştir. Simülasyon sonuçları, mevcut yerel taraf bilgi tabanlı yol seçimi (LSI-RS) ve rastgele yol seçimi (RRS) algoritmalarıyla karşılaştırıldığında, önerilen algoritmanın toplam gecikme, enerji verimliliği ve kullanımda üstün performanslara sahip olduğunu göstermektedir.

2.3.1. Örnek bir yazılım tanımlı akıllı şebeke mimari yapısı

Yazılım tanımlı akıllı şebeke mimarisine örnek olabilmesi açısından literatürdeki önemli çalışmalardan birinin mimari yapısı Şekil 2.4.'de sunulmuştur.



Şekil 2.4. Yazılım tanımlı akıllı şebeke mimarisi [1].

Bu mimari, optik ağlar, kablosuz sensör ağları ve araç-şebeke (V2G, Vehicle to grid) veya şebeke-araç (G2V, Grid to vehicle) ağları için önerilmiştir [1].

Bu tez çalışmasında, yukarıdaki mimari model örnek alınarak kendi kısıtlarımıza göre yeni bir mimari altyapı oluşturulmuştur.

2.4. IoT Temelli Akıllı Evler

IoT, farklı cihazların internet üzerinden birbirleriyle ve kullanıcılarla iletişim kurmasına olanak sağlayan bir teknoloji olarak tanımlanır [55]. IoT, insanların hayatlarını kolaylaştıran ve verimliliği arttıran birçok uygulama sunar. Nesnelerin interneti olarak da bilinen bu teknoloji, cihazlar arasında veri paylaşımını mümkün kılarak, farklı birçok endüstride ve sektörde kullanılmaktadır [56]. Bunlar arasında sağlık, enerji, otomotiv, üretim, tarım ve ev otomasyonu gibi alanlar yer alır. IoT cihazları, bu sektörlerdeki işlemlerin otomatikleştirilmesine ve verimliliğin artırılmasına yardımcı olur [57].

IoT teknolojisinin temeli, nesnelerin interneti için özelleştirilmiş birçok farklı özelliğe sahip cihazın kullanılmasıdır. IoT cihazları ile veri toplama, işleme, depolama ve paylaşım işlemleri gerçekleştirilir. Sensörler, aktüatörler, kameralar, akıllı telefonlar,

giyilebilir cihazlar ve araçlar gibi cihazlar IoT teknolojisiyle birbirine bağlanabilmektedir.

- Sensörler, fiziksel dünyadaki değişimleri algılayarak diğer cihazlara bilgi gönderir.
- Aktüatörler, sensörlerin algıladığı bilgilere göre hareket ederek fiziksel dünyada değişiklik yapar.
- Kameralar, nesnelerin interneti sayesinde diğer cihazlarla entegre olarak video görüntüleri gönderebilir ve alabilir [58].
- Akıllı telefonlar, IoT teknolojisi sayesinde birbirleriyle bağlanarak veri alışverişi yapabilir.
- Giyilebilir cihazlar, kullanıcının sağlık verilerini ölçerek diğer cihazlara aktarabilir [59].
- Araçlar, nesnelerin interneti aracılığıyla birbirleriyle haberleşerek trafik akışını iyileştirebilir [58].

Birçok sektörde hızla yaygınlaşan IoT teknolojisi, pek çok avantajı da beraberinde getirir. İlk olarak, IoT cihazları, sürekli veri akışı sağlayarak gerçek zamanlı analiz yapılmasına izin verir [54]. Bu sayede, hızlı kararlar alınarak, sorunlar daha hızlı çözülebilir. Ayrıca, IoT cihazları, insan müdahalesi olmadan otomatik olarak veri toplama, analiz ve işleme yapabilirler [58]. Böylece, insan hatası riskinin azalmasıyla zaman ve kaynak tasarrufu sağlanır [60]. Aynı zamanda, fiziksel dünyayı dijital dünya ile entegre ederek, daha iyi bir anlayış ve denetim sağlar [55]. Bu sayede, kaynakların daha verimli kullanılması ve israfın azaltılması mümkün olabilir. Bunun yanı sıra, bu teknolojiyle insanların yaşam kalitesi artırılabilir. Örneğin, akıllı sağlık cihazları, insanların sağlık durumunu izleyerek, daha iyi bir sağlık hizmeti sunabilir. Deniz ve okyanusların durumu ve çeşitli veriler hakkında hizmet sunan sensörler ve iletişim sistemleriyle balıkçılar, teknelerini yönetebilir. Böylelikle sanal bir dünyaya ait olan nesnelerin sağladığı hizmetle biz insanların dünyası haberdar edilebilir. Otonom uygulamalardan bir diğeri ise tarım alanlarında sıklıkla kullanılır. Bu sistemler sayesinde tarım alanlarını izleyen sensörler, hava durumu ve toprağın nem düzeyini analiz ederek gerekli durumlarda sulama sistemlerini çalıştırabilir. Ayrıca, geliştiriciler tarafından tamamen otonom uygulamalar ile merkezi mimariden bağımsız sistemler geliştirilebilir. Böylelikle bir doğal afet bölgesinde şebeke

bağlantısı olmayan, sensör özellikli cep telefonları ile ulaşılamayan yerlerdeki canlıların yerinin tespit edilmesi mümkün hale gelebilir [61].

Akıllı ev sistemleri de IoT uygulamalarındandır ve içindeki cihazların birbirleri arasında iletişim kurarak entegre bir şekilde çalıştığı bir ev olarak tanımlanabilir. IoT temelli akıllı evler, günümüzde artan internet kullanımı ve gelişen teknolojiler sayesinde hayatımızın bir parçası haline gelmiştir. Bu evler, ev sahiplerine ve kullanıcılara birçok avantaj sağlamaktadır [62].

IoT destekli ev otomasyon sistemlerine, akıllı aydınlatma, ısıtma, güvenlik sistemleri, hava/su kalitesi izleme, akıllı kilit sistemleri ve enerji yönetim sistemleri örnek verilebilir. Bu otomasyon sistemleri yaşam alanlarının kontrolünü kişiselleştirerek insan hayatını kolaylaştırmayı amaçlar. IoT cihazları sayesinde, ev sahipleri bu sistemleri uzaktan kontrol edebilir ve günlük hayatlarını kolaylaştırabilirler. Örneğin, enerji kullanımının akıllı termostat ile izlenebilir olması, evdeki sıcaklığı kontrol ederek enerji tüketimini optimize edebilir ve bu durum, ev sahiplerinin enerji tasarrufu sağlamalarına da yardımcı olabilir [63].

Kullanıcı müdahalesi olmadan insanların konforunu ve güvenliğini sağlayan bu uygulamalar genellikler sensörler ve aktüatörlerden oluşur. Evdeki cihazlara internet üzerinden bağlanarak çeşitli komutlar verilerek insan-makine (H2M, Human to machine) etkileşimi sağlanabileceği gibi duman sensörünün değerine göre aksiyon alıp alarmı çalıştıran bir senaryodaki gibi makine-makine (M2M, Machine to machine) etkileşimi de sağlanabilir [62].

IoT teknolojilerinin yaygınlaşması insan hayatında büyük kolaylıklar sağlasa da önlemlerin alınmaması durumunda güvenlik açıklarının oluşmasına ve çeşitli tehditlere yol açmaktadır. Akıllı ev otomasyon sistemlerinin yaygınlaşmasının beraberinde getirdiği bazı riskler, literatürdeki birçok çalışmada incelenmiştir [64]. IoT'nin doğası, her şeyin internete bağlanmasıdır ve bu da binlerce hatta milyonlarca cihazı yönetmek için gereken yasal ve teknik çerçevenin oldukça zorlu olduğu anlamına gelmektedir.

Bu sebeple, IoT sistemlerinin güvenliği konusu oldukça önemlidir. Gizlilik ve güvenlik riskleri, siber saldırılara maruz kalma riski, veri bütünlüğü sorunları ve ağ uyumluluğu sorunları dikkat edilmesi gereken riskler arasında yer alır [55]. IoT cihazları, internet üzerinden birbirlerine bağlanarak, bir ağ oluştururlar ve bu ağlara

yetkisiz kişilerin müdahalesi güvenlik riski oluşturabilir. Ayrıca, bu cihazlar arasındaki farklılıklar ve kullanılan farklı ağların güvenliği de IoT güvenliğini büyük ölçüde etkilemektedir.

Özellikle IoT temelli akıllı evler söz konusu olduğunda bu güvenlik sorunları büyük bir endişe kaynağıdır. Örneğin, siber saldırganlar evin kamera, hareket sensörü gibi güvenlik sistemlerini devre dışı bırakabilir ve evin kapısını açabilir. Böylece, ev sahiplerince hemen fark edilmeyecekleri bir hırsızlığa zemin hazırlayabilirler. Bunun yanı sıra, siber saldırganlar evin ısıtma veya soğutma sistemlerini kontrol edebilirler. Enerji faturalarını artırabilir veya daha da kötüsü ısıtma sisteminin manipüle edilmesiyle evde yangın çıkartılarak can ve mal kaybına sebep olabilirler [58].

Ayrıca, siber saldırganlar ev sahiplerinin kişisel verilerine de erişebilirler. Evdeki cihazlar, sürekli olarak veri toplar ve bu veriler siber saldırganlar tarafından ele geçirilebilir. Bu da ev sahiplerinin kişisel verilerinin tehlikeye girmesine neden olur [65]. Bu veriler, ev sahibinin hareketleri, tercihleri, alışkanlıkları, konum bilgisi ve hatta sağlık durumu hakkında bilgiler içerebilir. Örneğin, akıllı bir termostat, ev sahibinin evde ne zaman olduğunu, hangi sıcaklıkların tercih edildiğini ve belki de uyku düzeni hakkında bilgi toplayabilir. Benzer şekilde, akıllı bir güvenlik kamerası ev sahibinin evde ne zaman olduğunu, kimlerin geldiğini ve kimlerin ayrıldığını kaydedebilir. Siber saldırganlar elde ettikleri bu kişisel verileri dolandırıcılık veya şantaj amacıyla kullanabilir ve/veya üçüncü kişilerle paylaşabilirler.

Bu yüzden, IoT temelli akıllı evlerin güvenliği ve gizliliğini sağlamaya büyük önem verilmelidir. Buradan yola çıkarak, IoT cihazları için güçlü bir güvenlik çerçevesi oluşturmak, algılama, tanımlama, hizmet sağlama ve IT altyapısı gibi tüm aşamalar için kapsamlı bir koruma sağlamak gerekmektedir. Bununla birlikte, veri sızıntıları ve harici tehditler gibi birden fazla tehdit de göz önünde bulundurulmalıdır. Bu nedenle, güvenlik teknolojilerinin, sistem bileşenlerinin tüm seviyeleri için güçlü bir koruma sağlaması gerekmektedir, böylece IoT'nin avantajlarından yararlanırken güvenlik risklerini en aza indirmek mümkün hale gelebilir. Bu koruma yöntemleri arasında, cihazlar arasında güvenli kimlik doğrulama, veri şifreleme ve ağ güvenliği protokolleri kullanımı yer alabilir. Ayrıca, ev sahipleri düzenli olarak cihazlarının yazılımlarını güncellemeli ve zayıf noktaları kapatmak için siber güvenlik uzmanlarından yardım almalıdır.

Sonuç olarak, IoT temelli akıllı evler, kullanıcılar için birçok avantaj sağlamaktadır. Bu evler, ev sahiplerinin yaşam kalitesini yükseltirken, enerji tasarrufu sağlayabilir ve evdeki farklı sistemleri uzaktan kontrol etme imkanı sunarak günlük hayatı kolaylaştırabilir. Ancak diğer yandan IoT temelli akıllı evlerin güvenliği konusunda hala endişeler vardır [65, 67]. Kullanıcıların ve sistemlerin güvenliği için IoT cihazlarına karşı koruma önlemleri alınarak güvenlik ile ilgili endişelerin giderilmesi gereklidir. Bu sebeplerle IoT teknolojisi hakkında daha fazla araştırma yapılması, kullanıcıların ihtiyaçlarının daha iyi karşılanması, teknolojinin olası dezavantajlarını en aza indirilmesi ve güvenlik zafiyetlerinin giderilmesi gibi konularda çalışmalar ve geliştirmeler yapılmaya devam edilmelidir.

Son yıllarda IoT temelli akıllı evler oldukça popüler hale gelmiş ve bu konuda birçok araştırma yapılmıştır. IoT'nin sahip olduğu multidisipliner yapısı sonucunda akademik çalışmalar mimari tasarımdan siber güvenliğe, enerji verimliliğinden kriptolojiye kadar birçok alanı kapsamaktadır. Bu çalışmalardan bazıları Tablo 2.4.'de sunulmaktadır.

Tablo 2.4. Literatürdeki IoT temelli akıllı evler ile ilgili çalışmalar [66-68].

Başlık	Yayın Yılı	Özet
IoT-based smart homes: A review of system architecture, software, communications, privacy and security	2018	IoT temelli akıllı ev sistemleri için sistem mimarisi, yazılım, iletişim, gizlilik ve güvenlik konuları ele alınmaktadır. IoT teknolojisinin akıllı evlerde kullanımının avantajlarına ve akıllı ev cihazlarının çalışma prensiplerine değinilirken ayrıca, IoT teknolojisinin güvenlik açıkları, gizlilik ve uyumluluk sorunları da incelenmektedir.
Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes	2018	IoT tabanlı akıllı evlerin siber ve fiziksel güvenlik zafiyetlerinin değerlendirilmesine odaklanılmaktadır. Bu kapsamda, akıllı evlerin siber güvenlik riskleri, bunların nedenleri ve evin dışındaki tehditler gibi faktörler ele alınmıştır. Ardından, akıllı evlerin bu güvenlik açıklarını azaltmak için kullanılabilecek teknolojiler ve yöntemler anlatılmıştır.
A systematic review of the smart home literature: A user perspective	2019	Akıllı ev teknolojilerinin kullanıcının perspektifinden mevcut durumu incelenmiştir. Makale, akıllı evlerin kullanımının artmasına rağmen, kullanıcıların bu teknolojiye yönelik tutumlarının karmaşık olduğunu belirtmektedir. Bu soruna çözüm olarak akıllı evlerin kullanımının yaygınlaşması için kullanıcı ihtiyaçlarına odaklanılması gerektiği anlatılmıştır.

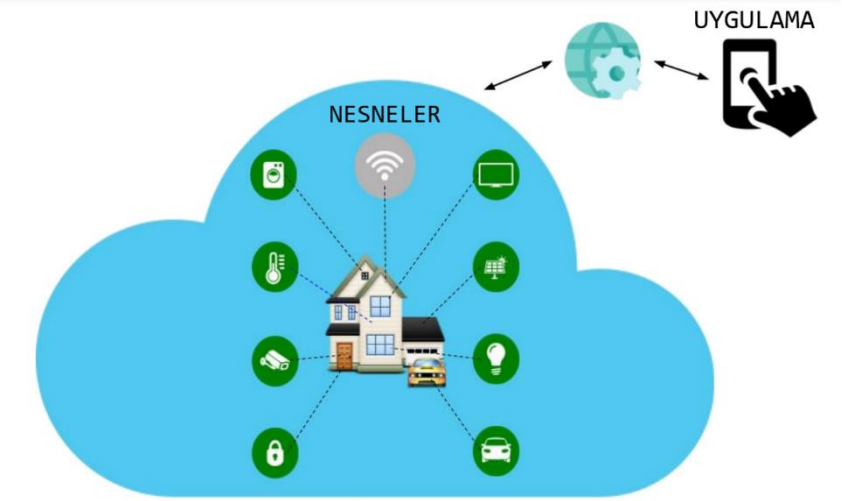
Tablo 2.4. (Devamı) Literatürdeki IoT temelli akıllı evler ile ilgili çalışmalar [69-71].

Başlık	Yayın Yılı	Özet
A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations	2020	IoT tabanlı akıllı ev uygulamalarında kullanılan yapay zeka yöntemlerini, bunların sınıflandırılmasını, avantajlarını, dezavantajlarını ve gelecekte karşılaşılması muhtemel zorluklarını ele almaktadır. Akıllı ev uygulamalarında yapay zeka tekniklerinin kullanımının artmasıyla birlikte karşılaşılan zorlukların anlaşılmasına ve gelecekte yapılacak araştırmaların yönlendirilmesine katkı sağlanmıştır.
An IoT-Based Smart Home Automation System	2021	IoT tabanlı akıllı ev otomasyon sistemlerine odaklanılarak sensörler, kontrol cihazları, ağ bağlantısı ve yazılım sistemlerinden oluşan bir mimari önerilmiştir. Sistem, akıllı ev cihazlarının uzaktan izlenmesine, kontrol edilmesine ve programlanmasına olanak tanımaktadır. Ayrıca, çeşitli testler gerçekleştirilerek sistemin güvenilir ve etkili olduğu kanıtlanmıştır.
Cybersecurity Threats and Countermeasures of the Smart Home Ecosystem	2022	Bu makale, akıllı ev cihazlarının nasıl çalıştığına ve akıllı evin güvenlik ve mahremiyet tehditlerine ışık tutmayı amaçlamaktadır. Akıllı ev ortamında kullanılabilecek bir güvenlik önlemi ile akıllı ev IoT tabanlı güvenlik protokollerinin bir karşılaştırması sunulmuştur.

2.4.1. Örnek bir IoT temelli akıllı ev mimari yapısı

Akıllı evler, insanların hayatlarını otomatize ederek kolaylaştırmak için geliştirilmiş sistemlerdir. Bu doğrultuda, oluşturulacak akıllı ev sisteminin kapsamı kullanıcının beklentisine ve ihtiyaçlarına yönelik değişiklik gösterebilir. Aşağıda, literatürdeki akıllı ev mimarilerinden biri anlatılmış olup akıllı ev mimarilerinin ihtiyaçlara yönelik değiştirilmesi ve/veya geliştirilmesi mümkündür.

Literatürdeki çalışmalardan birinin önerdiği akıllı ev mimari yapısı Şekil 2.5.'te verilmiştir. Bu mimaride kullanılan akıllı cihazlar/sistemler şunlardır: çamaşır makinesi, iklimlendirme, güvenlik kamerası, kapı sensörü, televizyon, güneş enerjisi paneli, aydınlatma, garaj kapısı.



Şekil 2.5. Akıllı ev mimarisi [72].

Ev içindeki akıllı cihazların birbirleriyle entegre çalışması, bir kontrol merkezinin varlığı ile mümkündür [72]. Akıllı cihazlar, yapılarındaki IoT donanımları ile elde ettikleri verileri kablosuz iletim yoluyla kontrol merkezine iletir. Verileri analiz eden ve işleyen kontrol merkezi, belirli kurallar çerçevesinde aksiyonlar alarak evin yönetimini sağlar. Bu yönüyle kontrol merkezi, bir akıllı evin beynidir denilebilir.

Bu kurallar, kullanıcı tarafından kendi isteklerine göre oluşturulur. Örneğin akıllı termostatın ölçtüğü sıcaklık verisi, kullanıcının önceden belirlediği aralıklara göre ısıtma veya soğutma sistemlerinin çalışmasını tetikleyebilir. Kullanıcı ve akıllı ev arasındaki bu etkileşim, mobil ve/veya web uygulamaları sayesinde gerçekleştirilir. Akıllı ev ile ilgili verileri toplayan kontrol merkezi, bunları işleyerek elde ettiği bilgileri uygulamaya gönderir. Uygulama aracılığı ile kullanıcıya bu bilgiler sunularak

evi hakkında detaylı bilgiye erişmesi sağlanmaktadır. Kullanıcı, yine bu uygulama aracılığı ile bir veya birkaç sisteme bağlı durumlarda alınacak aksiyona ait kuralları belirler.

Özellikle son yıllarda akıllı ev sistemlerinin gelişmesiyle birlikte kullanımı yaygınlaşmış ve yine bu doğrultuda yapılan çalışmaların sayısında da artış gözlenmiştir. Akıllı ev mimarileri ile ilgili literatürdeki çalışmalar incelendiğinde, kullanıcının talepleri doğrultusunda çok büyük ölçekli yapılar oluşturulabileceği gibi sadece bir cihazın veya sistemin yönetildiği küçük yapılar da oluşturulabilir. Bu bölümde anlatılmak üzere literatürdeki çalışmalardan biri seçilmiş olsa da bir akıllı ev mimarisinin kullanıcının talepleri doğrultusunda oluşturulduğu/belirlendiği unutulmamalıdır.

3. YAZILIM TANIMLI AĞLAR VE NESNELERİN İNTERNETİ TEMELLİ BİR AKILLI EV AĞI MİMARİ ÖNERİSİ

Akıllı evlerin popüler hale gelmesiyle birlikte, evlerde kullanılan akıllı cihaz sayısındaki artış, bu cihazların verimli bir şekilde yönetilmesini zorlaştıran bir problem olarak karşımıza çıkmaktadır. Bu problem, IoT teknolojisinin önemi ve gerekliliğinin gün geçtikçe arttığını göstermektedir.

Kullanıcılara, evlerinde bulunan akıllı cihazları uzaktan izleme ve yönetme; evdeki cihazlara, birbirleriyle haberleşme imkanı sağlayan IoT teknolojisi, enerji tüketimini optimize etmeye de yardımcı olmaktadır. Günümüzde akıllı şebekeler ile kullanıma sunulan ve enerji yönetiminde önemli bir araç olan akıllı sayaçlar, IoT teknolojisi ile kullanıldığında enerji yönetimi ve enerji tasarrufu konusunda önemli fırsatlar sunmaktadır. Bu teknolojilerle birlikte SDN teknolojisi de enerji şebekelerindeki ağ yönetimini daha etkili hale getirerek, enerji şirketlerinin enerji tüketimini ve dağıtımını yönetmesini kolaylaştırır.

Sonuç olarak, akıllı evlerin IoT teknolojisi ile yönetilmesi ve SDN temelli enerji şebekeleri ile desteklenmesi, enerji yönetimi ve tasarrufu konusunda önemli bir adımdır. Bu teknolojiler, enerji arzının sınırlı olduğu dünyamızda enerji tüketimini optimize etmek ve arz ve talep dengesini sağlamak için kullanılabilecek önemli araçlardır.

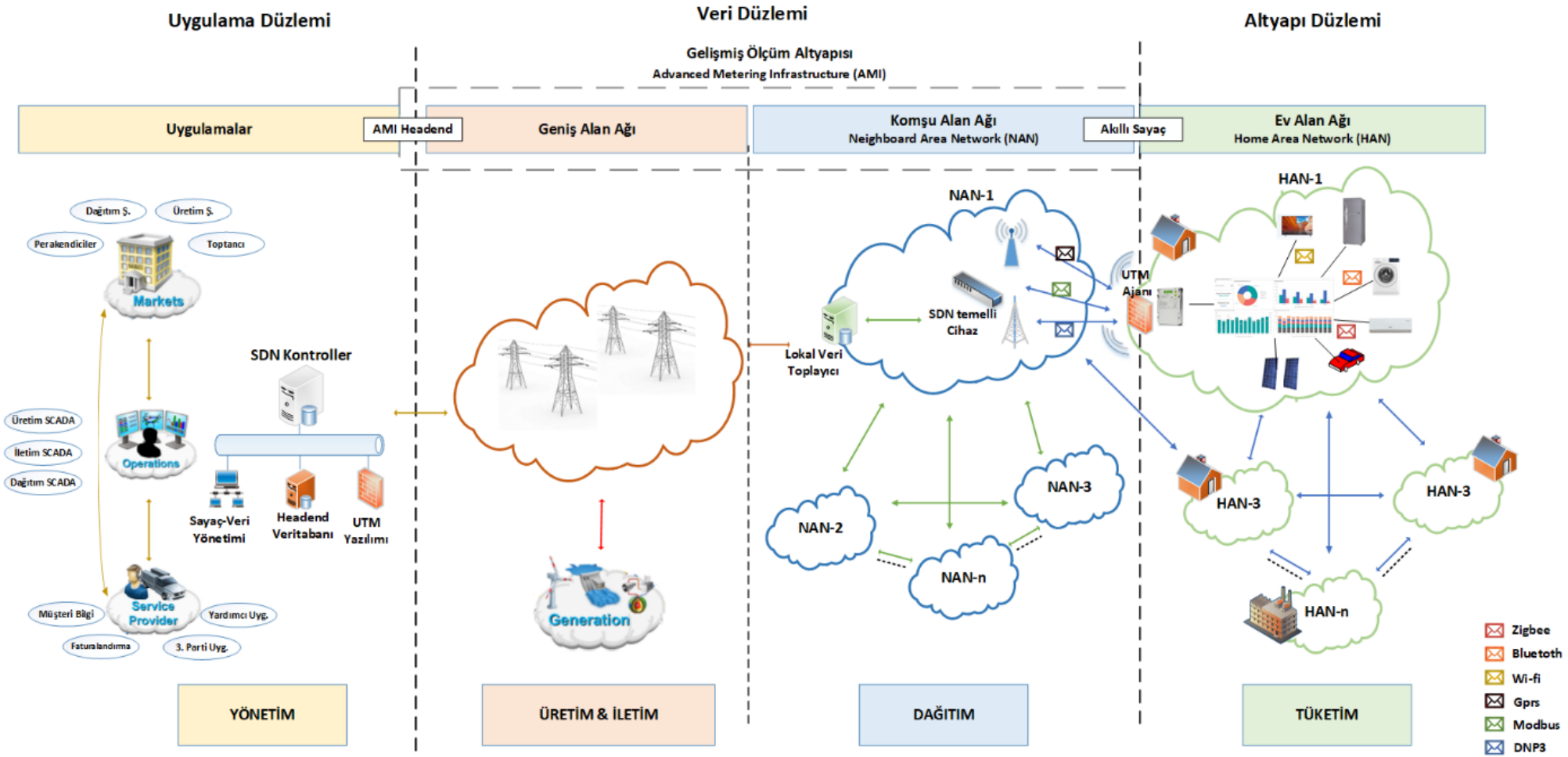
Bu tez çalışmasında, literatürdeki çalışmalar incelenerek eksiklikler saptanmış ve ardından bu sistemlerin entegre bir şekilde çalıştığı, günümüz ihtiyaçlarını karşılayabilecek yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı ev ağı mimarisi önerilmiştir. Bu kapsamda tezin bu bölümünde, ilk olarak önerilen yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı ev ağı mimarisinin gösterimi ile hakkında bilgiler verilecektir. Daha sonra bu mimarinin simülasyon ortamında nasıl gerçekleştirildiği anlatılacak ve son olarak oluşturulan ev ağının çalışmasına dair normal ve saldırı durumlarındaki senaryolar anlatılarak bu senaryoların gerçekleştirilmesiyle oluşturulan veri setlerinden bahsedilecektir.

3.1. Mimari Genel Bilgi

Bu tez çalışmasında önerilen yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı şebeke mimarisi Şekil 3.1.'de verilmiştir. Bu mimari yapıda, NIST'in önerdiği ve 7 bileşenden (üretim, iletim, dağıtım, tüketim, pazar, hizmet sağlayıcı, yönetim) oluşan akıllı şebeke yapısı SDN temelli olarak planlanmış ve tüketim domaini içerisindeki ev alan ağı (HAN), IoT temelli akıllı ev sistemi olarak tasarlanmıştır.

Tasarlanan mimariye göre, tüketim domainindeki akıllı evler SDN ağı ile enerji yönetim sistemine bağlanmaktadır. Merkezle akıllı evler arasındaki haberleşme WAN (Wide Area Network, Geniş alan ağı) ağını yöneten SDN kontrolör aracılığı ile gerçekleşmektedir. Akıllı evler, veri çıkış noktası olan akıllı sayaçlar ile SDN ağına katılırlar. Ev alan ağı içerisinde tüketilen ve üretilen enerji miktarları akıllı sayaçlar ile ölçülür ve SDN ağında bulunan ağ cihazları aracılığıyla merkeze gönderilir. Bu toplanan veriler ışığında yönetim domaininde bulunan enerji yönetim sistemi tarafından tüketim ve üretim miktarları analiz edilerek enerji talebi ve üretimi arasındaki dengesizliklerin önüne geçilip enerji kaynaklarının daha etkin bir şekilde kullanılması sağlanır.

Önerilen bu model, NIST tarafından önerilen akıllı şebeke mimarisinde ve literatürde kabul görmüş akıllı ev sistemlerine uygun şekilde tasarlanmıştır.



Şekil 3.1. Önerilen yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı şebeke mimarisi.

3.2. Modelleme ve Test Ortamı

Bu tez çalışmasında, önerilen yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı ev mimarisi simülasyon ortamında oluşturulmuş ve uygulanmıştır. Bu kapsamda, bu bölümde önce simülasyon ortamının oluşturulması, ardından da bu çerçevede oluşturulan IoT altyapısı 2 başlık altında anlatılacaktır.

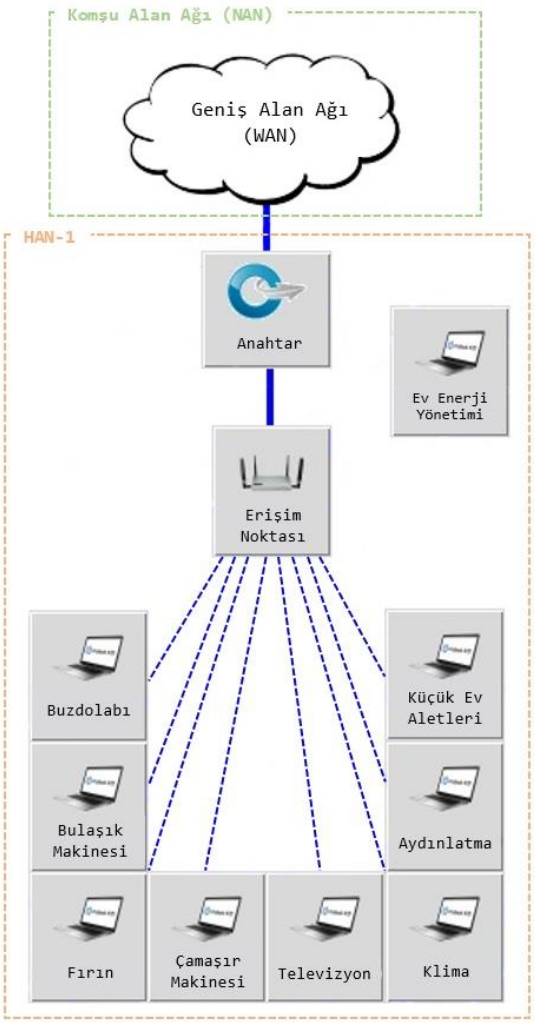
3.2.1. SDN altyapısının oluşturulması

Bu tez çalışmasında önerilen mimariyi gerçekleştirmek için Mininet isimli ağ sanallaştırma aracı kullanılmıştır. Mininet, Linux makine üzerinde çalışan bir Python uygulamasıdır. Bu uygulama, sanal ana bilgisayarlar (host), anahtarlar (switch) ve yönlendiriciler (router) içeren bir ağ topolojisi oluşturur. Bu sanal cihazlar, gerçek dünya cihazlarına benzer davranışlar sergilerler ve Mininet, bunların birbirleriyle nasıl etkileşime gireceğini simüle eder. Mininet, yazılım tanımlı ağları simüle etmek için oldukça kullanışlı bir araçtır. Bu nedenle, birçok ağ araştırmacısı ve endüstri profesyoneli, SDN uygulamalarını geliştirmek ve test etmek amacıyla Mininet'i kullanmaktadır. Mininet, OpenFlow protokolünü kullanarak, anahtarlar ve yönlendiriciler arasındaki iletişimi kontrol etmek için kontrolör görevi üstelenen bir yazılım kontrolcüsüyle (Ryu, Floodlight, POX vb.) birlikte çalışabilir. Bu, SDN uygulamalarının Mininet üzerinden test edilmesini sağlar [73].

Mininet, miniedit isimli bir grafik arayüze sahiptir. Miniedit, mininet simülasyonlarını daha hızlı ve anlaşılır şekilde oluşturmak için kullanılan bir araçtır. Bu araç sayesinde, görsel bir ara yüz kullanarak sanal ağlar oluşturulabilir, düzenlenebilir, ağların davranışları takip edilebilir ve yönetilebilir. Şekil 3.2.'de bu tez çalışmasında önerilen mimarinin miniedit arayüzü ile oluşturulmuş örnek modeli gösterilmektedir.

Önerilen yazılım tanımlı ağda bulunan nesnelerin interneti temelli akıllı ev mimarisinde, bir akıllı evdeki enerji tüketiminin simüle edilmesi için mininet platformu kullanılmıştır. Mimaride akıllı ev içinde bulunan beyaz eşyalar, küçük ev aletleri, iklimlendirme ve aydınlatma sistemleri gibi IoT destekli akıllı cihazları temsil etmek için birer sanal host oluşturulmuştur. Her bir host, aslında birer xterm yani uçbirim olarak çalışmaktadır. Xterm'ler üzerinde temsil ettiği cihaza ait kodlar çalıştırılarak, ilgili cihazın enerji tüketiminin taklit edilmesiyle simülasyon gerçekleştirilmektedir. Simülasyon ortamında 2 adet HAN yapısı oluşturulmuştur. Her bir HAN'da buzdolabı, bulaşık makinesi, fırın, çamaşır makinesi, televizyon, klima,

aydınlatma ve küçük ev aletleri olmak üzere toplam 8 adet akıllı ev cihazı modellenmiştir.



Şekil 3.2. Simülasyon ortamında oluşturulan akıllı ev topolojisi.

Geliştirilen python kodları sayesinde akıllı evdeki cihazlardan örneğin buzdolabının çalışma yapısı simülasyon ortamında taklit edilebilmektedir. Benzer kodlar her bir cihaz için kendi yapılarına uygun olacak şekilde geliştirilmiştir. Önerilen mimarideki akıllı evde modellenmesi planlanan cihazların yapısı ve detaylı bilgileri bölüm 3.2.2.1.'de anlatılmaktadır.

Literatürdeki çalışmalardan farklı olarak sabit özellikteki cihazlar seçmek yerine gerçek hayattaki kullanım durumlarının etkin bir şekilde yansıtılabilmesi amacıyla mimari, her bir cihaz için farklı özelliklere sahip olabilecekleri şekilde tasarlanmıştır. Bu yaklaşımdan yola çıkılarak, xterm çalıştırıldığında buzdolabının sahip olacağı özellikler, önceden belirlenen alanların sahip olabileceği değerlere göre rastgele bir

şekilde seçilir. Bütün özellikleri belirlenen buzdolabının enerji tüketimini hesaplayan host, ağa bu tüketim verisini gönderir. Böylelikle ağda bir buzdolabı çalışıyormuş gibi enerji tüketim verisi oluşturulmuş olur.

Bir cihaza ait sanal host, cihazın çalışmasını taklit ederek enerji tüketim değerini erişim noktası (access point) üzerinden SDN anahtar (switch) cihazına gönderir. Erişim noktasının bağlı olduğu SDN destekli anahtar cihazı, tüketim verilerini akıllı sayaca iletmekten sorumludur. Akıllı sayaca gelen tüketim verileri buradan enerji şebekesine iletilir. Akıllı sayaca gönderilen tüketim verisi aynı zamanda erişim noktası üzerinden HEM (Home Energy Management, Ev enerji yönetimi) yazılımı ile de paylaşılır.

HEM yazılımı, cihazlardan enerji tüketim verilerinin okunduğu ve kontrol paneli vasıtasıyla kullanıcı taleplerine göre yönetildiği bir sistemdir. Bu yazılım sayesinde kullanıcılara evlerindeki akıllı cihazların durumu ve enerji tüketimi hakkında detaylı bilgi verilmektedir. Böylece akıllı evin izlenebilirliği ve enerji tüketiminin yönetilebilir hale gelmesi sağlanmıştır.

Enerji tüketimindeki anomali durumları da HEM yazılımı sayesinde fark edilebilir. Tüketilen enerji değerlerinin gerçek zamanlı olarak izlenmesini sağlayan bu yazılım, aynı zamanda lokalinde bulunan veri tabanına bu verileri kaydeder. Çeşitli makine öğrenme algoritmalarıyla verileri analiz ederek anormal durumları tespit eden bir sistemi de bünyesinde barındırır. Böylelikle, akıllı ev sistemine yapılan bir siber saldırı ve/veya cihazların olağan çalışma düzeninden çıkması durumları kolaylıkla tespit edilebilir.

Anomali tespitinin HAN'da yapılmasının sebebi, akıllı şebeke yapısı içerisinde çok fazla sayıda uç düğümün yani abonenin olmasıdır. Bütün abone verilerinin merkezde analiz edilerek anomali tespitinin yapılması, günümüz teknolojilerinde performans açısından uygun ve mümkün bir yaklaşım değildir. Bu sebeple, bu akademik çalışmada tasarlanan mimari yapıda edge computing yaklaşımı benimsenmiştir.

Edge computing, IoT, IIoT, yapay zeka ve diğer benzeri teknolojilerin gelişmesiyle birlikte ortaya çıkmıştır. Veri işleme, depolama ve yönetimi için yeni bir yaklaşım sunar. Bu yaklaşımda, veriler bulut merkezlerine gönderilmeden önce ağ cihazları, kontrol cihazları veya diğer kaynaklar tarafından yakalanıp işlenir. Merkeze, ham veriler yerine işlenmiş verilerin gönderilmesi mantığına dayanan bu yaklaşım, ağ

trafiğini ve gecikmelerini azaltarak ağ ve hizmet performansını artırmayı amaçlar. Bir robot kolun kontrolü için kullanılan verilerin, fabrikadaki cihazlara gitmesine ve geri dönmesine gerek kalmadan yerel olarak işlenmesi, bu yaklaşımın gerçek hayattaki kullanımına örnek verilebilir [74-75].

Önerilen mimaride, edge computing yaklaşımının benimsenmesiyle, akıllı şebeke mimarisindeki yönetim ve üretim domainlerinin üzerine düşen yükün azaltılması hedeflenmiştir. Bu sebeple, akıllı ev içerisindeki enerji tüketim verilerinin anomali tespiti, HEM yazılımında yapılmaktadır. Merkeze sadece tespit sonucu yani normal-anormal etiketi ve toplam tüketilen enerji bilgisi gönderilmektedir.

3.2.2. IoT altyapısının oluşturulması

Tasarlanan yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı ev mimarisi, bir akıllı evde bulunabilecek beyaz eşyalar, küçük ev aletleri, aydınlatma ve iklimlendirme sistemlerinden oluşmaktadır. Bu sistemler, evdeki enerji tüketimini optimize etmeyi ve evin konforunu artırmayı amaçlamıştır.

Akıllı ev mimarisinin temeli veriye dayanır. Sistem, cihazlara ait verilere göre işleyişini yönlendirir. Bu sebeple akıllı ev sistemlerinde IoT destekli cihazlar kullanılması gerekmektedir. Cihazların IoT destekli olması onları akıllı hale getirir ve ihtiyaç halinde cihaz bilgilerine ulaşılmasını sağlar. Bunlara cihaz üzerindeki hareket sensör bilgisi, zamanlayıcı bilgisi, basınç bilgisi, sıcaklık bilgisi, nem bilgisi ve enerji tüketim bilgisi örnek verilebilir. Toplanan bu bilgilerin değerlendirilip çeşitli amaçlarla işlenmesi ve kullanıcının talepleri doğrultusunda sistemin geri beslenerek entegre bir şekilde işlemesi ve yönetilmesiyle akıllı ev yapısı oluşturulmuş olur.

Bir akıllı ev için bilgiyi elde etmek ne kadar önemliyse o bilgi ışığında aksiyon almak da bir o kadar önemlidir. Duman algılayan fakat alarmı ve söndürme sistemini çalıştırmayan bir yangın sisteminin hiçbir anlamı yoktur. Bu sebeple, toplanan verilerin kaydedilmesi, değerlendirilmesi ve işlenmesi süreçleri akıllı ev sisteminin temelini oluşturur. Evin kontrol noktası olarak da adlandırılabilecek bir yönetim sisteminin gerekliliği de buradan doğmaktadır. Cihazlar ve yönetim sistemi arasında bilgi akışını sağlamak için farklı protokoller kullanılır. Bu protokoller, cihazların birbirleriyle uyumlu bir şekilde çalışmasını sağlar. Bu IoT protokollerine Wi-Fi, Bluetooth, MQTT ve Zig-bee örnek verilebilir.

Bu bölümde ilk olarak bahsi geçen ve evde kullanılan makinelerin ve sistemlerin anlatımı yapılacak, ardından ev alan ağı içinde kullanılan protokoller hakkında genel bilgi verilerek tasarlanan mimaride kullanılan protokollerden bahsedilecektir.

3.2.2.1. Kullanılan cihazlar

Günümüzde akıllı cihazların çeşitliliği gün geçtikçe artmaktadır. Bu sayede, akıllı ev sistemleri bütünsel bir şekilde oluşturulabilir ve sistemlerin birbirleriyle entegrasyonu kolaylıkla sağlanabilir hale gelmiştir. Evin kapısında bulunan bir sensörle ev sahibinin eve geldiğinin anlaşılması ve gerekli saatlerde ışıkların otomatik olarak açılması veya evin sıcaklık değişimini takip eden bir akıllı termostatın, ölçüm değerine göre evin ısıtma sistemini otomatik olarak kontrol etmesi, entegre çalışan sistemlere örnek olarak gösterilebilir.

Bu tez çalışmasında önerilen akıllı ev mimarisi Şekil 3.3.'te gösterilmektedir. Bu mimari tasarlanırken günümüz evlerinin ihtiyaçları ve kullanıcıların beklentileri göz önünde bulundurulmuştur. Tasarlanan akıllı evdeki cihazlar şunlardır: Buzdolabı, bulaşık makinesi, fırın, çamaşır makinesi, televizyon, klima, aydınlatma/ampul, tost makinesi, kettle (su ısıtıcısı), elektrikli süpürge, ütü.

Şekil 3.3. Önerilen akıllı ev mimarisi [64].

Bu cihazlar seçilirken gerçek hayatı yansıtmak amacıyla ortalama bir evde bulunabilecek çeşitte beyaz eşyalar ve ev aletleri tercih edilmiştir. Akıllı evin yönetilmesi ve enerji tüketiminin izlenebilmesi için cihaz çeşidinin bilinmesi tek başına yeterli değildir. Örneğin, aynı özelliklerde iki çamaşır makinesi karşılaştırıldığında makinelerden birinin kapasitesi 7 kilodan 10 kiloya çıkartıldığında

iki makinenin tükettiği elektrik enerjileri değişmektedir. Bu sebeple, akıllı ev sisteminin doğru izlenebilmesi için evde kullanılan cihazlara ait detaylı bilgiye de sahip olunmalıdır.

Literatürdeki çalışmalardan farklı olarak sabit özellikteki cihazlar seçmek yerine gerçek hayattaki kullanım durumlarının etkin bir şekilde yansıtılabilmesi amacıyla mimari, her bir cihaz için farklı özelliklere sahip olabilecekleri şekilde tasarlanmıştır. Bu amaç doğrultusunda, piyasada en çok tercih edilen 5 markaya ait ürünlerin teknik dokümantasyonları ve kullanım kılavuzları detaylı şekilde incelenerek tasarlanan evde bulunan 8 farklı akıllı cihazın/sistemin sahip olabileceği özellikler belirlenmiştir. Daha sonra her evi yaklaşık olarak temsil edebilmek amacıyla, 5 farklı markaya ait aynı özellikteki cihazın enerji tüketim değerlerinin ortalaması alınarak ilgili cihazın nihai tüketim değerleri belirlenmiştir. Bu yoğun araştırmalar sonucunda elde edilen ürüne bilgileri ve enerji tüketim değerleri simülasyon ortamında kullanılmak üzere kaydedilmiştir.

Tezin bu bölümünde, kullanılan cihazlardan ve bahsi geçen özelliklerinden bahsedilecektir. Ayrıca, bahsi geçen özellikleri içeren cihaz özellik tabloları EK A'da da sunulmuştur.

Piyasada çok farklı özelliklerde buzdolapları olmasıyla birlikte bir buzdolabının tükettiği enerji değerini etkileyen üç temel özellikten bahsedilebilir. Bunlar, enerji sınıfı, hacim ve o buzdolabını kullanan kişi sayısı veya başka bir değişle evde yaşayan kişi sayısıdır. Piyasada çok farklı enerji sınıflarında buzdolapları olsa da günümüzdeki modellerde en sık rastlanan D, E ve F enerji sınıfları seçilmiştir. Hacim, buzdolabının en boy uzunluğuna ve 1, 2, 4 kapak olmasına göre farklılık gösterir. Bu çalışmada, buzdolapları kendi içinde 3 farklı hacimde sınıflandırılmıştır. Evde yaşayan kişi sayısı, günümüzdeki aile yapıları da göz önüne alınarak 1, 2, 3, 4 ve daha fazla şeklinde belirlenmiştir.

Bulaşık makinesi için enerji tüketim değerlerini etkileyen en önemli dört özellikten bahsedilebilir. Bunlar, enerji sınıfı, su tüketimi, program ve haftalık kullanım sayısıdır. Günümüzdeki bulaşık makinesi modellerinin en sık rastlandığı C, D ve E enerji sınıfları seçilmiştir. Farklı su tüketim değerlerine sahip bulaşık makineleri olsa da piyasada en sık görülen 9,5, 11,5 ve 12,9 litre su tüketim değeri olarak belirlenmiştir.

Program olarak en temel programlar olan yoğun, eko, hızlı ve ön yıkama programları seçilmiştir. Haftalık kullanım sayısı, 1, 2, 3, 4 ve daha fazla şeklinde belirlenmiştir.

Fırın için enerji tüketim değerlerini etkileyen en önemli dört özellikten bahsedilebilir. Bunlar, enerji sınıfı, tür, program ve haftalık kullanım sayısıdır. Günümüzde fırın modellerinde en sık rastlanan A ve B enerji sınıfları seçilmiştir. Ankastre fırın ve ocaklı fırın olmak üzere iki tür belirlenmiştir. Fırında pişirilen yiyeceklerin çeşidine göre süre ve sıcaklık ayarlandığından programlar et, tavuk, balık, sebze, kek, hamur işi şeklinde kategorize edilmiştir. Haftalık kullanım sayısı, 1, 2, 3, 4 ve daha fazla şeklinde belirlenmiştir.

Çamaşır makinesi için enerji tüketim değerlerini etkileyen en önemli beş özellikten bahsedilebilir. Bunlar, enerji sınıfı, hacim, devir, program ve haftalık kullanım sayısıdır. Günümüzde çamaşır makinesi modellerinde en sık rastlanan A, B ve C enerji sınıfları seçilmiştir. Hacim olarak 8, 9 ve 10 kg; devir olarak ise 1000, 1200 ve 1400 devir belirlenmiştir. Program olarak en sık kullanılan pamuklu, sentetik, eko ve hızlı programları tercih edilmiştir. Haftalık kullanım sayısı, 1, 2, 3, 4 ve daha fazla şeklinde belirlenmiştir.

Televizyon için enerji tüketim değerlerini etkileyen en önemli dört özellikten bahsedilebilir. Bunlar, enerji sınıfı, ekran tipi, ekran boyutu ve haftalık kullanım süresidir. Enerji sınıfı olarak E, F ve G sınıfları belirlenmiştir. Ekran tipi için günümüzde sık tercih edilen FHD ve 4K UHD ekranlar, ekran boyutu olarak ise 50, 55 ve 65 inç ekranlar tercih edilmiştir. Haftalık kullanım süresi için 1-4, 4-8, 8-12 ve 12+ olarak dört farklı saat aralığı belirlenmiştir.

Klima için enerji tüketim değerlerini etkileyen en önemli dört özellikten bahsedilebilir. Bunlar, enerji sınıfı, tür, ısıtma/soğutma kapasitesi ve haftalık kullanım süresidir. Enerji sınıfı olarak günümüz klimalarında en sık rastlanan A, B ve C enerji sınıfları seçilmiştir. Klimalar split, mobil ve salon tipi olmak üzere üç farklı türde kategorize edilmiştir. Isıtma/soğutma kapasitesi olarak 12000, 18000, 24000 BTU (British Thermal Unit, İngiliz ısı birimi) değerleri seçilmiştir. Haftalık kullanım süresi için 1-4, 4-8, 8-12 ve 12+ olarak dört farklı saat aralığı belirlenmiştir.

Aydınlatma elemanlarının enerji tüketim değerleri iki özelliğe bağlıdır. Bunlar, tür ve haftalık kullanım süresidir. Aydınlatma elemanları halojen, floresan ve led olmak

üzere üç türe ayrılmış ve haftalık kullanım süresi için 1-10, 10-20, 20-30 ve 30+ saat olarak dört farklı saat aralığı belirlenmiştir.

Küçük ev aleti olarak tost makinesi, kettle, ütü ve süpürge tercih edilmiş ve seviye 1, seviye 2, seviye 3 ve seviye 4 olmak üzere 4 farklı güç değeri belirlenmiştir. Haftalık kullanım süresi için 1-4, 4-7, 7-10 ve 10+ saat olarak dört farklı saat aralığı belirlenmiştir.

3.2.2.2. Kullanılan protokoller

Ev alan ağı içerisindeki IoT iletişiminde farklı protokoller kullanılabilmektedir. Günümüz akıllı ev sistemlerinde sıklıkla kullanılan Bluetooth, Wi-Fi, MQTT, CoAP, Zig-bee ve Z-Wave gibi protokoller bunlardan bazılarıdır. Kullanılan haberleşme protokolleri, cihazların iletişim kurduğu ağ teknolojisine ve kullanılan cihazların özelliklerine bağlı olarak belirlenir. Ayrıca, kullanıcı gereksinimleri, cihaz uyumluluğu, işlevselliği ve güvenliği de kullanılacak protokolün belirlenmesinde etkili unsurlardır. Örneğin, Zigbee pil ömrü uzun olan düşük güç tüketen cihazların olduğu ağlarda tercih edilirken, hızlı ve güvenli veri iletiminin gerçekleştirilmesi gereken ağlarda MQTT protokolü tercih edilir.

Tezin bu bölümünde ilk olarak literatürde en sık kullanılan Bluetooth, MQTT ve Zig-bee protokolleri anlatılacak, ardından önerilen mimaride tercih edilen Wi-Fi protokolü hakkında detaylı bilgi verilecektir.

Bluetooth, kablosuz iletişim söz konusu olduğunda akla gelen ilk protokollerdendir. Günümüzde genellikle kulaklık, fare, klavye, akıllı telefon ve tablet gibi cihazlarda kullanılır. Kısa menzilli kablosuz iletişim için tasarlanmıştır ve genellikle düşük güç tüketimi nedeniyle mobil cihazlar için tercih edilmektedir. Kablosuz cihazlar arasındaki iletişimi kurmak için bir eşleşme süreci kullanır. Bu süreçte, iki cihazın bağlantı kurabilmesi için birbirlerini tanıması ve eşleşmesi gerekir. Bu eşleşme sistemi, bluetooth teknolojisinin güvenli bağlantılar kurmasına olanak sağlar. Çoklu cihazlar arsında aynı anda iletişim kurma kabiliyeti başka bir avantajıdır ve çok kullanıcılı uygulamalarda bluetooth'un tercih edilmesini sağlar. Ancak bluetooth teknolojisinin dezavantajları da vardır. Kısa mesafeli bir kapsama alanına sahiptir ve veri transfer hızı diğer kablosuz iletişim protokollerine kıyasla düşüktür [76-78].

MQTT (Message Queuing Telemetry Transport), IoT uygulamaları için kullanılan basit, hafif ve güvenli bir mesajlaşma protokolüdür. Yaygın olarak sensör ağı, akıllı

evler ve endüstriyel IoT uygulamalarında kullanılır. TCP/IP üzerinde çalışır ve istemci-sunucu modelini kullanır. Bu modelde, istemci sunucuya bağlanarak belirli bir konuya abone olur veya mesaj gönderir. Sunucu, bir konuya yeni mesaj geldiğinde o konunun abonesi olan istemcilere bunu iletir. Bu yapısından dolayı düşük güç tüketimi, hızlı veri transferi ve güvenli iletişim sağlar. Bu özellikleri sebebiyle, IoT verilerinin toplanması ve yönetilmesi için ideal protokollerden biridir. Elbette bazı dezavantajları da vardır. Bunlardan biri, doğrudan cihazlar arasında iletişim sağlıyor olmasıdır. Bu durum, gerekli önlemler alınmazsa güvenliğin tam olarak sağlanamamasına sebep olabilir. Ayrıca, mesajların sunucu aracılığı ile iletilmesi, iletim gecikmelerine neden olabilir [79, 80].

Zig-bee, genellikle kablosuz sensör ağları ve akıllı ev uygulamalarında tercih edilen, açık kaynak kodlu kablosuz haberleşme protokolüdür. Düşük güç tüketimi, düşük maliyet ve düşük veri iletim hızı gibi özelliklere sahiptir. Bu yönüyle, diğer kablosuz teknolojilere göre birçok avantaj sağlamaktadır. ZigBee cihazları genellikle pil ile çalışır ve düşük güç tüketimi özelliği uzun pil ömrü sağlar. ZigBee cihazları ağa kolayca eklenebilir ve AES şifrelemesi kullandığından güvenli bir iletişim sağlar. Tüm bunların yanında bazı dezavantajları da vardır. Düşük veri hızına sahip olduğundan yüksek hızlı veri iletişimlerinde kullanılamaz. Ayrıca, veri iletim mesafesi diğer kablosuz protokollere kıyasla daha azdır [81-83].

WLAN'da (Wireless Local Area Network, Kablosuz yerel alan ağı) kullanmak üzere geliştirilen IEEE 802.11 standardı, ticari olarak Wi-Fi adıyla bilinir ve günümüzde günlük hayatın vazgeçilmezi haline gelmiştir. 2.4 ve 5 GHz bant genişliklerinde veri iletimi yapan teknolojinin temel amacı, kullanıcıların hem birbirlerine hem de internete kablosuz bağlanmalarını sağlamaktır. Wi-Fi ağları, bir veya daha fazla erişim noktası kullanılarak oluşturulur. Her cihaz, kablosuz sinyal yoluyla bir erişim noktasına bağlanarak iletişim kurar ve ağdaki diğer erişim noktaları da kendi aralarında iletişim kurabilir. Bu yapısı sayesinde kablosuz ağlar geniş bir alanda kullanılacak şekilde ölçeklenebilir. Wi-Fi ağları farklı veri aktarım modlarını kullanabilir. Örneğin, düşük maliyetli ve düşük güç tüketen cihazlar için 802.11b/g/n standardı uygunken, yüksek bant genişliğine sahip yüksek hızlı cihazlar için 802.11ac standardı uygundur [84].

Wi-Fi teknolojisi, akıllı cihazlara internet bağlantısı sağlamak, akıllı ev sistemleri, akıllı ulaşım sistemleri, endüstriyel otomasyon sistemlerinde veri iletimi sağlamak gibi

farklı alanlarda ve farklı uygulamalarda kullanıma uygundur. Kolay kurulum, mobilite, esneklik ve düşük maliyet gibi avantajlarından dolayı birçok alana yayılmıştır. Kablosuz iletişimi destekleyen herhangi bir cihazla uyumludur ve herhangi bir kablolama gerektirmediğinden kolay kurulur. Kablosuz bir teknoloji olduğundan cihazların konumları değişse bile kullanılmaya devam edilebilir. Bu özellik, insanların farklı mekanlarda internete erişimini kolaylaştırır. Bu kolaylık hem mobilite hem de esneklik özelliği ile açıklanabilir. Diğer yandan, kablolu ağlarda kablo döşeme ve tesisat işlemleri için ek maliyetler gerektiğinden, Wi-Fi teknolojisi çok daha ucuz bir seçenektir [78].

Tüm bunların yanında bazı dezavantajları da vardır. Örneğin, Wi-Fi ağlarındaki birçok faktör bağlantı hızını etkileyebileceğinden kablolu ağlarla kıyaslandığında daha yavaş bir bağlantı hızına sahip olabilir. Bu durum, çevresel faktörlere olan hassasiyeti ile de ilişkilendirilebilir. Duvarlar, metal nesneler veya diğer kablosuz cihazlar Wi-Fi sinyalini zayıflatabilir veya engelleyebilir. Ayrıca, sinyal karışıklığı, bağlantı problemleri veya kapsama alanı problemleri yaşanabilir. Aynı frekansta çalışan Wi-Fi ağlarının birlikte kullanılması, sinyal karışıklığına neden olarak bağlantı hızını yavaşlatabilir. Kablosuz veri iletimi sağlayan bir teknoloji olduğundan güvenlik açıklarına sahip olabilir. Bunun önüne geçmek için Wi-Fi şifreleme teknolojileri kullanılsa da doğru şekilde yapılandırılmadığı sürece tam güvenlik sağlamaz. Bu dezavantajlar, Wi-Fi teknolojisinin avantajlarını gölgede bırakmaz, ancak kullanıcıların Wi-Fi kullanımlarına bu faktörleri göz önünde bulundurarak yaklaşmaları gerektiğini gösterir.

Bu tez çalışmasında önerilen yazılım tanımlı akıllı şebeke mimarisinde, HAN içindeki iletişimin sağlanması için Wi-Fi protokolü tercih edilmiştir. Hem literatürdeki çalışmalarda tercih edilen bir protokol olması hem günümüz akıllı ev sistemlerinde kullanıldığından gerçek hayatta da karşılığının olması hem de bu tez çalışmasında kullanılan Mininet simülasyon programında entegrasyonunun sağlanabilmesi sebebiyle bu protokol seçilmiştir.

Akıllı ev içindeki iletişim, cihazların verilerini Wi-Fi ile akıllı ev sisteminin izlendiği ve yönetildiği HEM yazılımına göndermesiyle kurulur. Örneğin, çamaşır makinesi, üretmiş olduğu verileri Wi-Fi paket yapısının içine ekleyerek ve HEM yazılımına gönderir. Bütün cihazlar benzer bir yapıda verilerini göndermektedir. Tek fark, cihazların, paket yapısının veri bölümünü kendi özelliklerine göre doldurmasıdır.

Belirli aralıklarla bu verilerin HEM yazılımına iletilmesiyle akıllı evin anlık izlenmesi sağlanır.

3.3. Senaryoların ve Veri Setlerinin Oluşturulması

Bu tez çalışmasında önerilen akıllı ev mimarisi, gerçek hayattaki örneklerine benzer çalışacak şekilde tasarlanmıştır. Bu benzerliğin sağlanmasını sağlayacak kilit nokta, tasarımın gerçeklenmesinde kullanılan senaryolardır. Literatürdeki çalışmalardan farklı olarak, belirli özelliklere sahip tek bir akıllı evin modellenmesi yerine, belirli kısıtlar çerçevesinde, gerçek hayatta karşılaşılması mümkün olan bütün akıllı ev senaryolarının modellenebileceği bir yaklaşım sunulmuştur.

Bölüm 3.2.1.'de oluşturulan akıllı ev ağı modelinin gerçeklenmesi için çeşitli senaryolara ihtiyaç duyulması sebebiyle, bölüm 3.2.2.1.'de bahsedilen, cihazların özellikleri kısıtları dikkate alınarak, simülasyonda kullanılacak senaryolar oluşturulmuştur.

Bu bölümde, tasarlanan akıllı ev mimarisinin simüle edilmesinde kullanılacak normal durumlara ait senaryolardan bahsedilecektir.

3.3.1. Normal durumlardaki ev senaryolarının oluşturulması

Her ev, sahibine özeldir ve onun ihtiyaçları ve hayat tarzı çerçevesinde belirli dinamiklere sahiptir. Örneğin, 5 kişilik bir ailenin evinde haftada 4 defa çamaşır makinesi çalıştırılıyor olabilir veya 2 kişilik bir aile, haftada 9 saat televizyon izliyor olabilir. Son derece öznel olan bu veriler aynı zamanda belirli bir sürekliliğe de sahip değildir. Örneğin, aynı 5 kişilik aile bir sonraki hafta 1 defa çamaşır makinesi çalıştırabilir veya aynı 2 kişilik aile, 16 saat televizyon izleyebilir. Hayatın akışında karşılaşılan bu düzensiz yapıya dikkat edilerek, bu tez çalışmasının gerçeklenmesinde kullanılacak ev senaryoları belirlenmiştir. Bu senaryolar bölüm 3.2.2.1.'de verilen, cihazların sahip olabilecekleri özelliklere dikkat edilerek oluşturulmuş ve evin modellenmesinde 8 cihaz için kullanılacak değerlere karar verilmiştir.

Örneğin bir evde, C enerji sınıfına sahip 9,5 litre su tüketen bir bulaşık makinesi haftada 2 defa yoğun programda çalışabilir ve bu çalışma sonucunda belirli bir enerji tüketimi gerçekleştirir. İşte bu kullanım şekli, o akıllı evin enerji tüketiminin modellenebilmesi için önceden belirlenmelidir. Diğer 7 cihaz için de kendi

özelliklerine uygun kullanım şekillerinin belirlenmesiyle, akıllı evin enerji tüketim senaryosu oluşturulmuş olur.

Belirlenen bu senaryo çerçevesinde simülasyon ortamındaki modelin çalıştırılmasıyla, düğümler ilgili cihaz gibi davranır ve akıllı ev, gerçeğe en yakın haliyle gerçeklenmiş olur. Örneğin, seçilen A enerji sınıfındaki klima diğer özellikleri aynı kalmak üzere, B enerji sınıfındaki bir klimayla değiştirilirse artık burada bambaşka bir senaryodan bahsedilmesi gerekir. İki senaryo birbirine benzerdir fakat aynı değildir. Bu, cihazların enerji tüketim değerlerinin, her bir özelliğinin etkisi altında olmasından kaynaklanır.

Her bir senaryonun oluşması için 8 cihazın özellik bilgilerine ihtiyaç vardır ve cihazların sahip olduğu toplam özellik sayısı 29'dur. Yani, birbirinden farklı her senaryo, 29 çeşit özelliğin benzersiz şekilde kombinasyonuyla oluşturulur. Bu kombinasyon sayısı 3.851.755.393.646.592 olarak hesaplanır. Bu sayı aynı zamanda, geliştirilen mimari tasarım ile simüle edilebilecek, birbirinden farklı akıllı evlerin de sayısıdır.

3.3.2. Veri setlerinin oluşturulması

Bu tez çalışmasının bir çıktısı olarak sunulan CSGEC-23 (Center Smart Grid Energy Consumption 2023) veri setleri, oluşturulan senaryoların simülasyon ortamında modellenmesiyle elde edilen çıktılar kullanılarak üretilmiştir. Mimaride kullanılan cihazların özellikleri gereği 755 milyarı aşkın farklı senaryo sayısı mevcut olsa da kullanılabilirliği artırmak amacıyla simülasyon ortamında 2 milyon farklı senaryo gerçekleştirilerek çıktıları kullanılmıştır.

Gerçeklenecek senaryoların seçimi, geliştirilen kodlar sayesinde yapılmış ve cihazların özellik kombinasyonlarının tekrarlı oluşmamasına son derece özen gösterilmiştir. Oluşturulan senaryonun benzersizliği ve rastgeleliği, kod içinde yapılan kontroller ile garantiye alınmıştır. Daha sonra, belirlenen senaryolar simülasyon ortamında gerçeklenerek enerji tüketim değerleri elde edilmiştir.

Bu bölümde, ilk olarak akıllı ev sisteminin normal işleyişindeki enerji tüketim değerleri kullanılarak bir veri seti oluşturulmasından bahsedilecektir. Ardından, sistemin siber saldırı altındayken ürettiği veriler kullanılarak anomali içeren başka bir veri setinin oluşturulması anlatılacaktır.

3.3.2.1. Normal durumlardaki veri seti

Model, belirlenen senaryolar kapsamında çalıştırıldığında, simülasyon ortamındaki düğümler temsil ettikleri cihaz gibi davranarak, kendi özelliklerini ve tükettikleri enerji değerini HEM yazılımına gönderir. Gönderilen bu veriler, akıllı evin çalışma durumunun ve bunun sonucunda tükettiği elektrik enerjisinin takip edilebilmesi amacıyla HEM yazılımının lokalindeki veri tabanında saklanır. Bu tez çalışmasında, bahsi geçen veri tabanındaki verilerin işlenerek yeni bir veri seti üretilmesi, bir çıktı olarak hedeflenmiştir.

Bu amaç doğrultusunda, veri setinin bulunacağı Excel dosyası oluşturularak, her cihaz için, sahip olduğu özellikler ve o özelliklerdeki enerji tüketim bilgilerinin tutulacağı sütunlar tanımlanmıştır. 8 cihaz türü için de sütunlar belirlendikten sonra toplam enerji tüketimi için de ekstra bir sütun oluşturulmuştur. En sonda ise anomali tespitinin sonucunda normal/anormal etiketlemesi için bir sütun oluşturulmuştur.

Her sütuna ilgili değer gelecek şekilde veriler doldurularak ilerlenir. Örneğin, akıllı evdeki buzdolabı için sahip olduğu enerji sınıfı, hacim ve evde yaşan kişi sayısı bilgileri ile bu özelliklerdeki buzdolabının harcadığı elektrik enerjisi değeri veri setine işlenir. Bu, bulaşık makinesi, fırın, çamaşır makinesi, televizyon, klima, aydınlatma ve küçük ev aletleri için teker teker uygulanır. Ardından, tüm cihazların tüketim değerleri toplanarak evin genel tüketimi bulunur ve son olarak normal/anormal etiketi eklenir.

Veri setinin her bir satırı, oluşturulmuş bir senaryoya karşılık gelmektedir. Daha önce oluşturulmuş olan 2 milyon senaryoya ait veriler doğruluğu bozulmamış şekilde “normal” olarak etiketlenerek veri seti oluşturulmuştur.

3.3.2.2. Saldırı durumlarındaki veri seti

Akıllı ev ağı, normal işleyişini gerçekleştirirken beklenmedik bir anda siber saldırıya uğrayabilir ve saldırganların veri manipülasyonuna maruz kalabilir. Böyle bir durumun yaşanması halinde verilerde yaşanabilecek manipülasyonun ağa olan etkilerini yansıtabilmek amacıyla ikinci bir veri seti daha oluşturulmuştur. Bu veri setinin ileride yapılacak çalışmalara katkı sağlaması hedeflenmektedir.

Bir saldırgan, ev ağına sızarak trafiği dinleyebilir ve yanlış veri enjeksiyonu (false data injection) saldırısı gerçekleştirerek verileri manipüle edebilir. Böyle bir durumda tüketim verileri değiştirilebileceği gibi cihazların özelliklerine ait veriler de

değiştirilebilir. Her iki anomali de sistemin güvenliği, bütünlüğü ve sürekliliği gibi kritik unsurları etkilediğinden saldırı tespit sistemleri tarafından fark edilerek sistemin güvenliği sağlanmalıdır. Yapılabilecek saldırılar bunlarla da sınırlı değildir. Gerçek hayattaki IoT sistemlerine ve akıllı evlere yapılan siber saldırılar incelendiğinde saldırganların tercih ettikleri saldırı türlerinin çok çeşitli olduğu görülmektedir. SQL Injection, DoS, Scanning ve Malware saldırıları bunlardan bazılarıdır.

Literatürdeki ve gerçek hayattaki siber saldırılar incelendiğinde, IoT sistemlerine ve akıllı evlere yapılan saldırılar belirlenerek bu tez çalışmasının bir çıktısı olan, saldırı altındaki akıllı eve ait enerji tüketim veri seti oluşturulmuştur. Bu veri setinde kullanılan saldırılar şunlardır: MITM (ortadaki adam saldırısı), yanlış veri enjeksiyonu (false data injection), tekrarlama saldırısı (masquerade attack). Ev içindeki makinelerden birinin saldırgan makineye dönüştürüldüğü düşünülerek, diğer ev aletlerinin HEM yazılımına gönderdiği veriler bu saldırılar ile manipüle edilmiştir. Bu veriler anormal olarak etiketlenerek veri setine eklenmiştir. %10, %20, %30 ve %40'lık anomali oranlarına sahip veri setlerinde toplam 2 milyon adet akıllı ev verisi bulunmaktadır.

4. MAKİNE ÖĞRENME ALGORİTMALARIYLA PERFORMANS ANALİZİ

Tez çalışmasının bu bölümünde, elde edilen veri setine uygulanan makine öğrenme algoritmalarının performans karşılaştırması yapılacaktır. Bunun için ilk önce veri setlerine uygulanan veri ön işleme tekniklerinden bahsedilecek, ardından kullanılan makine öğrenme algoritmaları açıklanarak RapidMiner programı kullanılarak veri setlerine uygulandığında elde edilen sonuçlar paylaşılacaktır. Son olarak ise genel bir karşılaştırma niteliğinde, makine öğrenme algoritmalarının performansları değerlendirilecektir.

4.1. Veri Ön İşleme

Dünya çapında hızla artan veri boyutları, bu verilerin analiz edilmesi ve işlenmesi gibi süreçleri kolaylaştıracak çözümler geliştirilmesine zemin hazırlamıştır. Buna yönelik olarak geliştirilen makine öğrenme teknikleri, verilerdeki gürültüye, eksikliklere ve uyumsuzluklara oldukça duyarlıdır ve bu durum performansı olumsuz etkiler. Daha doğru, etkili ve güvenilir sonuçlar elde edebilmek için makine öğrenme tekniklerinin uygulanmasından önce verilerin bir dizi işlemden geçirilmesi gerekliliği de buradan ortaya çıkmıştır. Bu ihtiyaca yönelik geliştirilen veri ön işleme, sisteme sunulacak verilerin kalitesini artırmak için eksik değerlerin atanması ve aykırı değerlerin çıkartılması gibi bazı teknikleri ifade eder [85].

Veri ön işleme, literatürde kendisine geniş yer bulmuş bir kavram olmakla birlikte, veri setinin mevcut durumu ve beklenen sistem çıktısına göre farklı adımlardan oluşmaktadır. Bu tez çalışmasında, veri setinin mevcut ihtiyaçları göz önüne alınarak veri ön işleme adımlarından, veri temizleme, veri azaltma, veri ölçeklendirme ve veri bölümlendirme teknikleri seçilmiştir.

4.1.1. Veri temizleme

Veri setinde eksik değerlerin olması, kullanılan makine öğrenme algoritmasının performansını doğrudan etkileyen bir durumdur. Buna çözüm olarak uygulanabilecek iki yöntem bulunmaktadır. Bunlardan ilki, eksik değerlerin tüm veri setine oranı önemsiz olduğunda uygulanabilecek, eksik değerli verilerin atılmasıdır. Makine

öğrenme algoritmalarının çoğu eksik değere sahip verileri işleyemediğinden az sayıdaki durumlarda bu yöntem uygulanabilir. İkinci yöntem ise eksik olan değerlerin tamamlanmasıdır. Eksik değere sahip veriler atılamayacak kadar çok olduğunda tercih edilen bu yöntem, çeşitli tamamlama yöntemleri kullanılarak tahmini değerlerle eksik verileri tamamlamayı kapsar [85].

Bu tamamlama yöntemleri kendi içinde tek değişkenli ve çok değişkenli yöntemler olarak ikiye ayrılabilir. Tek değişkenli yöntemler, ortalama değer tamamlama olarak özetlenebilir. Bu yöntemde, verideki eksik değerler sadece o değişkene ait özelliklere göre tahmin edilir. Tek değişkenli olarak isimlendirilmesi de buradan gelmektedir. Eksik değerin, o değişkenin ortalaması veya medyanı ile değiştirilmesi tekniği, tek değişkenli yöntemlere örnek gösterilse de uygun değerler üretmeyebilir. Bu konuda literatürde, zaman serisi metodu ve hareketli ortalama yönteminin kullanımı üzerine yapılan çalışmalar da mevcuttur [86]. Bu çalışmalar göstermektedir ki, eksik değerlerin tüm veri setine oranı düşük olduğunda (örneğin %1-5) tek değişkenli yöntemlerin kullanılması uygundur. Eksik değerlerin oranı daha yüksek olduğunda ise çok değişkenli yöntemlerin kullanılması gerekmektedir. K-en yakın komşu (KNN) algoritması ve regresyon tabanlı modeller çok değişkenli yöntemlere örnek verilebilir. Çok değişkenli yöntemlerdeki esas amaç, eksik değerin benzer veri örneklerinden yola çıkarak tamamlanmasıdır. Bu yöntem, eksik veri oranı fazla olan (örneğin %5-15) veri setlerine uygulandığında bile performansı tatmin edici düzeyde iyileştirdiği görülmüştür [87, 88].

Literatürdeki çalışmalar da göstermektedir ki, eksik verileri yerine koymak için mutlak bir çözüm belirlenememektedir. Veri setinin boyutu, eksik değer miktarı, hesaplama maliyeti gibi parametreler göz önünde bulundurularak seçilecek yönteme karar verilmelidir.

Bu tez çalışmasında, gerçekleştirilen saldırı senaryolarına bağlı olarak akıllı ev aletlerinin HEM yazılımına veri göndermemeleri durumu dikkate alınarak veri setinde oluşabilecek olası eksik değerlerin, kullanılan makine öğrenme algoritmalarının performansını azaltmaması için veri temizleme tekniği uygulanmıştır.

4.1.2. Veri azaltma

Veri seti boyutunun satır veya sütun bazında sayıca fazla olması makine öğrenme performansını olumsuz yönde etkileyebilecek durumlardandır. Böyle bir durumda veri

ön işleme adımlarından veri azaltma tekniği uygulanılması gerekmektedir. Veri azaltma, satır bazında veri örneği azaltma veya sütun bazında özellik değişkeni azaltma şeklinde iki yönde gerçekleştirilebilir. Her iki azaltma yöntemi için de uygulanan farklı teknikler mevcuttur.

Satır bazında veri azaltma için kullanılabilecek en basit teknik olan rastgele seçim, adından da anlaşılacağı üzere veri seti içinden tamamen rastgele şekilde örneklem belirlenen bir tekniktir. Çok büyük veri setlerinde kullanımı performans yönünden olumlu olsa da kritik verilerin elenme ihtimali, makine öğrenme sürecine olumsuz yansıyarak genel performansı düşürebilir. Diğer bir teknik olan tabakalı örnekleme, kategorilerdeki belirli oranı koruyarak örneklem belirleme işlemidir. Örneğin, orijinal veri setinde 150 adet normal ve 50 adet anormal olarak iki kategoriye ait veri bulunsun. Bu verilere %60 seçim oranıyla tabakalı örnekleme uygulanırsa, normal verilerin 90'ı ve anormal verilerin 30'u seçilecektir. Bu yöntemle, kategori kaybı olmaksızın veri azaltma uygulanabilmektedir [87].

Diğer bir yön olan sütun bazında veri azaltma için literatürde kabul görmüş üç yöntem bulunmaktadır. Birinci yöntem, değişkenler içinde istenilenleri doğrudan seçmektir. İkinci yöntem, öznitelik seçim tekniklerini kullanarak değişkenleri seçmektir. Bu teknikler kendi içinde 3 gruba ayrılır. Bunlar, hedef ve öznitelik arasındaki ilişkiyi istatistiksel temelli ele alan filtreleme (Filter) teknikleri, öznitelikleri kendi içinde alt gruplara bölerek performansını değerlendiren sarmalayıcı (Wrapper) teknikler ve model eğitiminin sağladığı optimizasyonla öznitelik seçimi yapan gömülü (Embedded) tekniklerdir [85]. Son olarak üçüncü yöntem ise öznitelik çıkarma tekniklerini kullanarak kullanışlı değişkenleri belirlemek amacıyla kullanışlı olmayanların çıkartılmasıdır. Bu üç teknikten hangisinin seçileceğinin kararı, veri setinin özelliklerine ve beklenen çıktıya bağlı olarak sağladıkları avantajlar ve dezavantajlar göz önüne alınarak verilmelidir.

Bu tez çalışmasında, akıllı ev aletlerinden elde edilen verilerin işlenmesi ve analizi süreçlerindeki performansı artırmak amacıyla, oluşturulan veri seti üzerinde satır bazında rastgele seçim yöntemiyle veri azaltma tekniği uygulanmıştır.

4.1.3. Veri ölçeklendirme

Veri setinde bulunan değişkenlerin ölçekleri (değerleri, boyutları) arasındaki olası farklılıklar, kullanılan makine öğrenme algoritmalarının bu değişkenleri analiz

etmelerinde çeşitli yanılgılar yaşamasına sebep olur. Örneğin kişilerin yaş ve gelir bilgilerini içeren bir veri setinde yaş aralığı 0-90, gelir miktarı 0-150 bin TL arasındaki değerleri içeriyor olsun. Böyle bir veri setinde uzaklık temelli hesaplamalar yapan Öklid gibi algoritmalar kullanıldığında değerlerde sapma gözlemlenebilir. Bu durumun önüne geçerek değişkenler arasındaki ölçüm farklılığını gidermek amacıyla veri ölçeklendirme teknikleri kullanılmaktadır. Bu tekniklerle, veriler arasındaki büyüklük/küçüklük algısında karışıklık olmadan model tarafından eşit şartlarda değerlendirilmesi mümkün hale getirilmektedir.

Veri ölçeklendirme teknikleri kendi içinde üç gruba ayrılabilir. Değişken değerlerini 0-1 aralığına dönüştürmek için maks-min normalizasyonu (aralık dönüşümü), ortalama değer 0 standart sapma 1 olacak şekilde değişkeni normal dağılıma getiren z-puan standardizasyonu ve son olarak veri değişkenlerinin farklılıklarını azaltmak amacıyla ondalık yapılarının taşındığı ondalık ölçek normalleştirme tekniği [85].

Bu tez çalışmasında, oluşturulan veri setindeki değişkenlerin boyutları arasındaki farklılığı azaltarak makine öğrenme algoritmalarının performansını artırmak amacıyla maks-min normalizasyonu yöntemiyle veri ölçeklendirme tekniği uygulanmıştır.

4.1.4. Veri bölümlendirme

Veri bölümlendirme, makine öğrenme algoritmaları ile çeşitli analizlerin yapılabilmesi için veriyi birkaç gruba ayırmayı amaçlar. Bu teknik sayesinde model eğitildikten sonra performansının değerlendirilebilmesi için bir test seti elde edilmiş olur. Bölümlendirmenin oranı ve yapısı, katı kurallar ile sınırlandırılmamıştır. Modelin çalışma şekli, veri setinin boyutu ve özellikler, istenilen çıktı gibi farklı beklentilere göre bölümlendirme işlemi şekillendirilmektedir. Yaygın bir kullanım olan, verinin %70 eğitim %30 test şeklinde bölümlendirilmesi, yaklaşımın açıklanması için örnek verilebilir. Bununla birlikte veri, eğitim, doğrulama ve test şeklinde üç farklı gruba da bölünebilir. Bölümlendirme işlemi yapılırken veri setinin karıştırılarak rastgele şekilde seçim yapılması gerekmektedir. Böylelikle, oluşturulan yeni gruplar birbirinden bağımsız ve veri setine ait özellikleri içerir hale gelir.

Literatürdeki çalışmalar incelendiğinde, veri bölümlendirme tekniğinin model performansını artırmaya yardımcı olabileceği görülmüştür. Ayrıca bu teknik, modelin gerçek veriler üzerindeki performansını objektif bir şekilde değerlendirmeyi sağlarken modelin aşırı öğrenmesi gibi sorunların önüne geçilmesine de yardımcı olur.

Bu tez çalışmasında oluşturulan veri setindeki veriler, %70 eğitim %30 test verisi olacak şekilde bölünmüştür. %75-25, %60-40 gibi farklı yaygın kullanım şekilleri olsa da %70-30 bölümlendirmesinin daha iyi performans gösterdiği görüldüğünden bu yöntem tercih edilmiştir.

Bu tez çalışmasında anlatılan bölümler ve literatürde incelenen çalışmalar sonucunda Tablo 4.1.'de veri setlerinin karşılaştırması verilmiştir. Ardından, bu tez çalışmasında tercih edilen makine öğrenme algoritmalarının performans karşılaştırması sunulacaktır.

Tablo 4.1. Literatürdeki veri setlerinin karşılaştırması [105, 106].

Veri Seti	Açıklama	Veri Sayısı	Anomali (%)	Saldırı Çeşitleri	Kullanılan Makine Öğrenme Algoritmaları
UNSW-NB15	Veri kümesinin ham ağ paketleri, gerçek, normal etkinlikler ile sentetik çağdaş saldırı davranışlarının bir melezini oluşturmak amacıyla UNSW Canberra'nın Siber Menzil Laboratuvarında oluşturulmuştur.	2.540.044	12,64	• Fuzzers • Analysis • Backdoors • DoS • Exploits • Generic • Reconnaissance • Shellcode • Worms	• Naïve Bayes (NB) • Decision Tree (DT) • Artificial NeuralNetwork (ANN) • Logistic Regression (LR) • Expectation-Maximization (EM) • Clustering
CIDDS-001	Küçük bir işletme ortamı taklit edilerek zararsız kullanıcı davranışlarını içeren normal etkinlikler ile kötü amaçlı trafiği içeren veri kümelerinin oluşturulması için bir yaklaşım önerilmiştir.	4.194.300	2,94	• DoS • Brute Force • Port Taramaları	-

Tablo 4.1. (Devamı) Literatürdeki veri setlerinin karşılaştırması [107, 108].

Veri Seti	Açıklama	Veri Sayısı	Anomali (%)	Saldırı Çeşitleri	Kullanılan Makine Öğrenme Algoritmaları
CIC-IDS-2017	Zaman damgası, kaynak ve hedef IP'ler, kaynak ve hedef bağlantı noktaları, protokoller ve saldırı temelinde etiketlenmiş, gerçek dünya verilerine benzer şekilde oluşturulmuş veri seti.	-	-	• DoS/ DDoS • Brute Force • XSS • SQL Injection • Infiltration • Port tarama • Botnet	• K-Nearest Neighbors (KNN) • Random Forest • Iterative Dichotomiser 3 (ID3) • Adaboost • Multi-layer Perceptron (MLP) • Naive Bayes • Quadratic Discriminant Analysis (QDA)
TON_IoT	Makine/Derin Öğrenme algoritmalarına dayalı farklı siber güvenlik uygulamalarının doğruluğunu ve verimliliğini değerlendirmek amacıyla oluşturulmuş IoT/IIoT veri kümeleri.	3.270.022	16,12	• DoS/ DDoS • Injection • MITM • Password • Ransomware • Scanning • XSS	• Support Vector Machines (SVM) • k-Nearest Neighbour (kNN) • Naïve Bayes (NB) • Random Forest (RF) • Classification and Regression Trees (CART) • Logistics Regression (LR) • Linear Discriminant Analysis (LDA)

Tablo 4.1. (Devamı) Literatürdeki veri setlerinin karşılaştırması [109].

Veri Seti	Açıklama	Veri Sayısı	Anomali (%)	Saldırı Çeşitleri	Kullanılan Makine Öğrenme Algoritmaları
NSL-KDD	KDD'99 veri setinin yapısındaki bazı sorunları çözmek için önerilen bir veri setidir. İzinsiz giriş tespit yöntemlerinin karşılaştırılmasına yardımcı olmak için etkili bir kıyaslama veri seti olarak kullanılabilir.	-	-	-	• J48 (decision tree learning) • Naive Bayes • NB Tree • Random Forest • Random Tree • Multi-layer Perceptron • Support Vector Machine (SVM)
CSGEC-23	Nesnelerin interneti temelli akıllı şebekelerde ev alan ağı içindeki akıllı cihazların enerji tüketimlerini içeren, gerçek dünya verileriyle oluşturulmuş veri seti.	2.000.000	10, 20, 30, 40	• MITM • False Data Injection • Masquerade Attack	• K-Nearest Neighbors (KNN) • Support Vector Machine (SVM) • Decision Tree • Random Forest • Naive Bayes • Artificial Neural Networks

4.2. Kullanılan Makine Öğrenme Algoritmalarının Performans Analizi

Günümüzde teknolojinin gelişmesi ve yaygınlaşmasıyla birlikte dünya genelinde üretilen veri miktarında hızlı bir artış görülmektedir. Birçok kurum ve akademik çalışma, bu konuyla alakalı bilgi ve belge sunmaktadır. Örneğin, DOMO'ya göre 2022 yılında bir dakikada gönderilen e-posta sayısı 231 milyon, sms sayısı ise 16 milyondur. Sosyal medyada ise dakikada 66 bin Instagram fotoğrafı, 347 bin tweet ve 1,7 milyon Facebook içeriği paylaşılmaktadır [89]. Veri miktarındaki bu artışa karşın bu verinin insanlar tarafından analiz edilmesi ve işlenmesi gün geçtikçe daha güç hale gelmektedir. Bu nedenle, büyük veri setlerinin analiz edilmesi, işlenmesi ve hedeflenen çıktıya ulaşılması gibi görevlerde makine öğrenme tekniklerinin kullanımı yaygınlaşmıştır. Günümüzde, sağlıktan ekonomiye, eğitimden siber güvenliğe, tarımdan otomotive kadar pek çok alanda ve sektörde makine öğrenme teknikleri kullanılmaktadır. Bu multidisipliner kullanım yapısı, farklı veriler, analizler, çıktılar, istekler ve beklentiler anlamına gelmektedir. Bu durum, makine öğrenme algoritmalarının sektör veya veri bazlı geliştirilmesine ve çeşitlenmesine yol açmıştır.

Makine öğrenme algoritmalarının çeşitliliği, kullanılacak algoritmanın seçim sürecinin de önemini artırmıştır. Hangi makine öğrenme algoritmasının kullanılacağı kararı, sektör verisinin türü, veri setinin özellikleri ve hedeflenen çıktı gibi faktörlere bağlıdır. Örneğin, veri setinin boyutu bu kararın alınmasında önemli bir unsurdur. Küçük veri setleri için genellikle basit algoritmalar yeterli olurken, büyük veri setleri için çok daha karmaşık algoritmalara ihtiyaç duyulabilir. Diğer yandan veri setinin çıktısı da algoritma seçiminde önemli bir faktördür. Örneğin, sınıflandırma problemleri için farklı algoritmalar tercih edilirken, regresyon problemlerinde farklı algoritmalar tercih edilebilir. Bu sebeplerle, bu tez çalışmasında yapılacak olan performans karşılaştırmasında kullanılacak algoritmaların seçiminde, oluşturulan veri setlerinin özellikleri dikkate alınmıştır.

Bu bölümde, ilk olarak seçilen algoritmaların performans karşılaştırmasında kullanılacak metrikler anlatılacak ve daha sonra, bu tez çalışmasının bir çıktısı olan veri setleri için kullanılacak olan makine öğrenme algoritmalarından bahsedilecektir. Her algoritmanın yapısı ve özellikleri anlatılıp veri seti üzerinde çalıştırıldığında elde edilen sonuçlar sunulacaktır.

4.2.1. Performans analizi için kullanılan metrikler

Makine öğrenme algoritmalarının performansını objektif bir şekilde değerlendirmek ve karşılaştırmalarını yapabilmek için bazı metrikler kullanılmaktadır. Çalışmanın bu bölümünde, performans karşılaştırmasında kullanılacak metriklerden bahsedilecektir.

Kullanılan makine öğrenme algoritmalarının başarım değerlendirmesi için Karışıklık Matrisi tekniği kullanılmıştır. Bu teknik ile elde edilen FP (False Positive – Yanlış Pozitif), FN (False Negative – Yanlış Negatif), TP (True Positive – Doğru Pozitif) ve TN (True Negative – Doğru Negatif) değerleri, daha sonra Doğruluk (Accuracy), Duyarlılık (Recall), Kesinlik (Precision) ve F1 Ölçütü (F1 Score) parametrelerinin elde edilmesinde kullanılmıştır. Tablo 4.2.'de verilen karışıklık matrisi, algoritmanın öngördüğü değerin gerçek değerler ile 4 farklı kombinasyonunu içeren bir çeşit tablodur.

Tablo 4.2. Karışıklık matrisi.

		Tahmini Değer	
		Doğru	Yanlış
Gerçek Değer	Doğru	TP	FN
	Yanlış	FP	TN

Bu tablonun parametreleri olan FP, FN, TP ve TN terimleri, verinin normal/anormal sınıflandırması kapsamında şu şekilde açıklanabilir:

FP: veri analizinin gerçek sonucu anormal iken makinenin o veriyi normal olarak sınıflandırması.

FN: veri analizinin gerçek sonucu normal iken makinenin o veriyi anormal olarak sınıflandırması.

TP: veri analizinin gerçek sonucu normal iken makinenin o veriyi normal olarak sınıflandırması.

TN: veri analizinin gerçek sonucu anormal iken makinenin o veriyi anormal olarak sınıflandırması.

Bu değerler kullanılarak makine öğrenme algoritmalarının, doğruluk, duyarlılık, kesinlik ve F1 skor gibi performans değerlendirme metrikleri elde edilir.

Doğruluk, algoritmanın doğru şekilde yaptığı sınıflandırmanın yüzdesidir. Algoritmanın ne kadar doğru sonuç vermeyi başardığını ortaya koyar. Denklem 4.1'de verilen şekilde hesaplanır.

$$\text{Doğruluk (Accuracy)} = \frac{\text{TP} + \text{TN}}{\text{TN} + \text{TP} + \text{FN} + \text{FP}} \tag{4.1}$$

Duyarlılık, algoritmanın pozitif olarak değerlendirmesi gereken verinin kaç tanesini pozitif olarak bulduğunun analizidir. "Gerçek pozitiflerin ne kadarı pozitif olarak değerlendirildi?" sorusunun cevabı aranır da denilebilir. Denklem 4.2'de verilen şekilde hesaplanır.

$$\text{Duyarlılık (Recall)} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4.2}$$

Kesinlik, algoritmanın yaptığı değerlendirmenin ne kadar doğru olduğunun analiz edilmesidir. Pozitif şekilde etiketlenen çıktıların gerçekte kaç adedinin pozitif olduğunu ortaya koyar. Denklem 4.3'te verilen şekilde hesaplanır.

$$\text{Kesinlik (Precision)} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{4.3}$$

F1 Ölçütü, duyarlılık ve kesinlik değerlerinin harmonik ortalamasıdır. Bir algoritma çıktısının doğruluğunun ölçütüdür ve minimum 0, maksimum 1 (tamamen kesinlik) değerlerini alır. Denklem 4.4'te verilen şekilde hesaplanır.

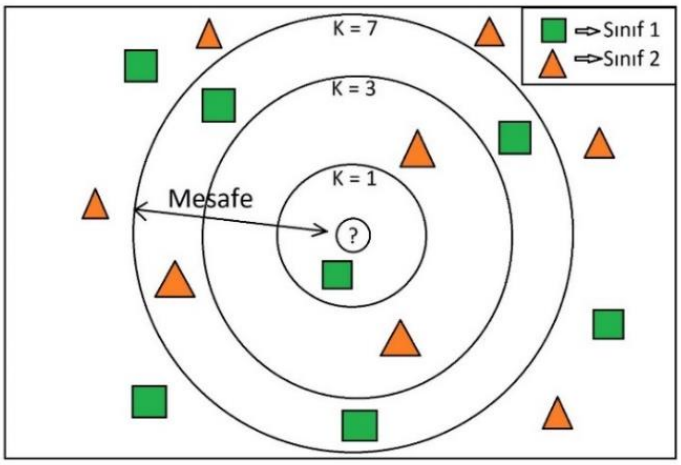
$$\text{F1 Ölçütü (F1 Score)} = \frac{2 \text{ x Duyarlılık x Kesinlik}}{\text{Duyarlılık} + \text{Kesinlik}} \tag{4.4}$$

4.2.2. Kullanılan makine öğrenme algoritmaları

4.2.2.1. En yakın komşu

Literatürde kısaca KNN (K-Nearest Neighbors) olarak da bilinen en yakın komşu algoritması, denetimli makine öğrenme algoritmalarından biridir. Uygulanması çok basit olduğu için sınıflandırma ve regresyon problemlerinde yaygın olarak kullanılır. Bu basitliği nedeniyle, veri madenciliğinden tıpa, örüntü tanımadan istatistiğe çok

farklı alanlarda kullanılmaktadır. Algoritmanın temeli, sınıflandırması yapılacak verilerin, eğitim kümesinden öğrenilen veriler ile benzerliğinin hesaplanarak, örnekleme en yakın olan k adet verinin ortalaması ile elde edilen eşiğe göre sınıflama yapılmasına dayanır. Bu çalışma yapısından dolayı, sınıflandırma yaparken belirlenecek karar sınırı, karmaşık veriler ile başa çıkmak için esneklik sağlayabilir [90].



Şekil 4.1. En yakın komşu algoritması modeli [92].

Basit bir KNN sınıflandırma modeli örneği Şekil 4.1.'de verilmiştir. Bu örneğe göre, eğitim kümesinden öğrenilen verilerden sınıf 1'de olanlar kare ile, sınıf 2'de olanlar üçgen ile belirtilmiştir. Yeni bir veri sınıflandırmak üzere algoritmaya sokulmuştur. K komşu değeri, k = 3 olarak atanır ise bu yeni veri sınıf 2 olarak sınıflandırılır çünkü belirlenen çemberin içinde 2 üçgen ve 1 kare bulunmaktadır. Eğer, k = 7 olarak atanır ise yeni veri sınıf 1 olarak sınıflandırılır çünkü belirlenen çemberin içinde 4 kare ve 2 üçgen bulunmaktadır.

Komşuluk sayısı k belirlenirken çift sayı olmamasına dikkat edilmelidir. Bunun sebebi, az bir ihtimalle bile olsa komşu sayısının çift sayı belirlenmesi durumunda sınıfların aynı uzaklıkta olma ihtimalidir. Bu çalışmada, k = 3, k = 5 ve k = 7 olmak üzere üç farklı komşuluk sayısında testler yapılarak KNN algoritmasının performansının ideal değerini bulmak amaçlanmıştır.

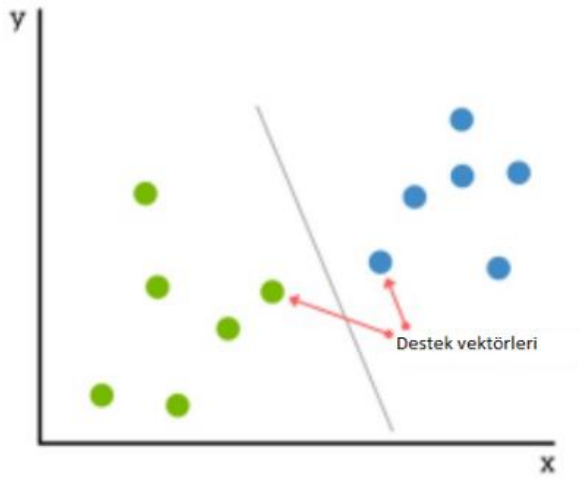
KNN algoritması, RapidMiner programı ile veri setlerine uygulanmıştır. K = 5 değeri için algoritmanın yaptığı sınıflandırma sonrasındaki başarım değerleri Tablo 4.3.'deki gibidir.

Tablo 4.3. En yakın komşu algoritması için test sonuçları.

Anomali Oranı	Doğruluk	Duyarlılık	Kesinlik	F1 Ölçütü
%10	89,32	99,15	90	94,35
%20	76,53	94,23	79,99	86,53
%30	63,48	83,69	70	76,23
%40	53,54	68,16	59,92	63,78

4.2.2.2. Destek vektör makineleri

Destek vektör makineleri yani kısaca SVM (Support Vector Machine), sınıflandırma ve regresyon için kullanılan bir makine öğrenme algoritmasıdır. Veri setinin sınıflandırmasında değişkenlerin bağlantısının bilinmediği durumlarda kullanılmak üzere önerilmiştir. Temel amacı, sınıfları doğru bir şekilde belirleyerek karar sınırı çizmek ve yeni gelecek örneklerin hangi sınıfa ait olduğunu tahmin etmektir [91]. Bunun için SVM, bir özellik uzayında veri noktalarını haritalayarak bu uzayda bir hiperdüzlem bulmaya çalışır. Hiperdüzlem, sınıflar arasında ayrım yapmayı sağlayan bir karar sınırı olarak da ifade edilebilir. Oluşturulan hiperdüzlem, veriyi iki veya daha fazla sınıfa ayırarak sınıflandırma işlemini gerçekleştirir. Sınıflandırmanın doğru şekilde yapılabilmesi için karar sınırı çizilirken düzlemdeki her sınıfa en uzak olan yer belirlenmelidir [92]. Örnek bir SVM uzayı Şekil 4.2.'de verilmiştir.



Şekil 4.2. Destek vektör makinesi algoritması modeli.

SVM, eğitim veri setindeki örneklerden yola çıkarak nesneleri doğru bir şekilde sınıflandırmayı amaçlar. Bunun için öncelikle eğitim veri setindeki giriş örneklerini ve sahip oldukları sınıf etiketlerini inceler. Örneğin, bir saldırı tespit sistemi için eğitim veri seti, bir ağ trafiğinin normal veya anormal olarak etiketlenmiş kayıtlarını içerir. Daha sonra, eğitim verilerini birbirinden ayırmak için en doğru konumdaki karar sınırını belirleyerek bir model oluşturur. Bu model, test veri setindeki yeni örneklerin sınıflandırılmasında kullanılır. Örneğin, yeni bir ağ trafiği verisi bu modele sokularak karar sınırına göre hangi sınıfa ait olduğu tahmin edilir [93].

Bu tez çalışmasında, SVM algoritması RapidMiner programı ile veri setlerine uygulanmıştır. Uygulama sonucunda oluşan modelin sınıflandırma başarım değerleri Tablo 4.4.'deki gibidir.

Tablo 4.4. Destek vektör makinesi algoritması için test sonuçları.

Anomali Oranı	Doğruluk	Duyarlılık	Kesinlik	F1 Ölçütü
%10	90	100	90	94,74
%20	80	100	80	88,8
%30	70	100	70	82,35
%40	60	100	60	75

4.2.2.3. Karar ağaçları

Karar ağaçları, sınıflandırma ve regresyon problemlerinde sık kullanılan bir denetimli makine öğrenme algoritmasıdır. Genellikle veri madenciliği üzerinde kullanılan bu yöntem, öznitelik düğümleri oluşturarak birtakım parametreye göre veriyi sürekli olarak ikiye bölme sürecinde dayanır [94]. Bu süreç, bütün veri sınıflandırılana kadar tekrar edilir.

Karar ağacı ismini modelin ağaç görünümünde olmasından alır. Düğümlerden en üstte bulunanı "kök düğüm" olarak isimlendirilir. Ağacın en sonundaki düğümler "yaprak" olarak isimlendirilir ve kök düğüme, arada bulunan "dal" düğümler ile bağlanır. Verinin bazı özelliklere göre test edilmesine kök düğümde başlanır ve her düğümdeki test sonucuna göre ilgili düğüm dallara ayrılır. Test sonucu kategoriktir yani evet/hayır gibi sonuçlar içerir. Bu test işlemi aşağıya doğru devam ederek ağaç şekline benzeyen

bir akış diyagramı oluşturur. Diyagramın en sonunda bulunan yaprak düğüme gelindiğinde nihai karara varılmış demektir [95].

Bu tez çalışmasında, karar ağacı algoritması RapidMiner programı ile veri setlerine uygulanmıştır. Uygulama sonucunda oluşan modelin sınıflandırma başarım değerleri Tablo 4.5.'deki gibidir.

Tablo 4.5. Karar ağaçları algoritması için test sonuçları.

Anomali Oranı	Doğruluk	Duyarlılık	Kesinlik	F1 Ölçütü
%10	90,03	100	90,03	94,75
%20	80,07	100	80,06	88,93
%30	70,26	100	70,18	82,48
%40	60,89	100	60,54	75,42

4.2.2.4. Rastgele orman

Rastgele orman, birleşik (ensemble) bir makine öğrenme algoritmasıdır. Bu yöntem, birden fazla karar ağacının, sınıflandırma başarımının artırılması amacıyla veri kümesinin rastgele seçilmiş alt kümeleri üzerinde eğitilmesi temeline dayanır. Her ağaç, veri kümesinin bir alt kümesiyle çalışır ve daha sonra tüm bu ağaçların çıktıları birleştirilerek son tahminler yapılır. Sınıflandırma problemlerinde, çoğunluk oyu kullanılarak en sık tahmin edilen sınıf belirlenir. Regresyon problemlerinde ise ağaçların tahmin değerlerinin ortalaması alınarak son tahmin yapılır [96]. Küçük ve basit ağaçlara ayrılması, istenildiği kadar ağaç oluşturulabilmesi, hata tahminini hızlı ve yüksek doğrulukta yapması gibi avantajlarından dolayı literatürdeki diğer sınıflandırma ve regresyon algoritmaları ile karşılaştırıldığında çok daha iyi sonuç vermektedir [97].

Bu tez çalışmasında, rastgele orman algoritması RapidMiner programı ile veri setlerine uygulanmıştır. Uygulama sonucunda oluşan modelin sınıflandırma başarım değerleri Tablo 4.6.'deki gibidir.

Tablo 4.6. Rastgele orman algoritması için test sonuçları.

Anomali Oranı	Doğruluk	Duyarlılık	Kesinlik	F1 Ölçütü
%10	90,16	100	90,15	94,82
%20	80,44	100	80,36	89,11
%30	70,76	100	70,54	82,72
%40	61,19	100	60,72	75,56

4.2.2.5. Naïve bayes

Naive bayes, Bayes teoremine dayanan istatistik temelli bir sınıflandırma algoritmasıdır. Veri kümesi içindeki verileri belirli olasılık hesaplarına göre kategorize etmeyi yani sınıflandırmayı amaçlar. Bunu, sisteme sunulan her veri için sahip olabileceği durumların olasılığını hesaplayarak yapar. Olasılık değerlerinden hangisi daha yüksekse, veri o sınıfa aittir kararını alır [98]. Bu algoritmada sisteme sunulan öğrenme verileri belirli bir kategoriye göre etiketlenmiş olmalıdır. Sisteme sunulan test verileri, öğrenme verilerinde yapılmış olasılıksal işlemler sonucuna göre değerlendirilerek sınıflandırılır. Bu sınıflandırmanın kesinliği, öğrenme verisinin sayısı arttıkça artmaktadır. Hızlı hesaplama kabiliyeti ve basit yapısı sayesinde literatürde sık kullanılan algoritmalardan olan naive bayes, metin sınıflandırması, duygu analizi ve spam filtreleme gibi konularda başarısını kanıtlamıştır [99, 100].

Algoritmanın temelinin dayandığı Bayes teoreminin matematiksel ifadesi Denklem 4.5'te verilmiştir.

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{4.5}$$

Denklemdeki A ve B olaylardır. Bu olayların birbirinden bağımsız şekilde gerçekleşme olasılıkları P(A) ve P(B) şeklinde ifade edilir. P(A|B), şartlı koşul ifadesidir yani B verildiğinde A'nın olma olasılığını temsil eder. Benzer şekilde P(B|A) ifadesi ise A verildiğinde B'nin olma olasılığını temsil etmektedir [101].

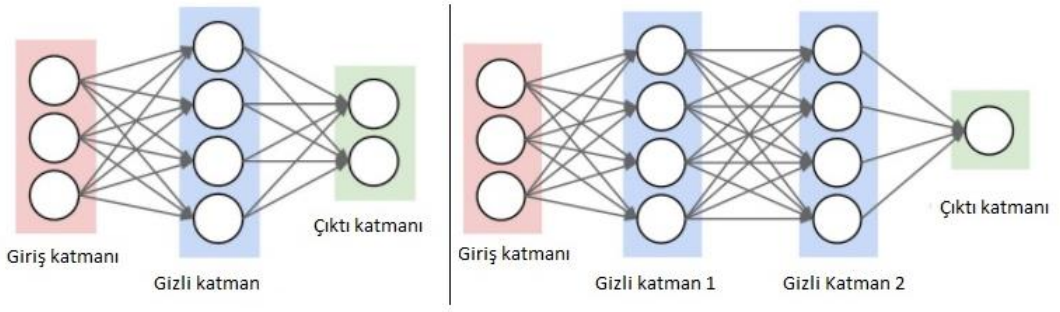
Bu tez çalışmasında, naive bayes algoritması RapidMiner programı ile veri setlerine uygulanmıştır. Uygulama sonucunda oluşan modelin sınıflandırma başarım değerleri Tablo 4.7.'deki gibidir.

Tablo 4.7. Naïve bayes algoritması için test sonuçları.

Anomali Oranı	Doğruluk	Duyarlılık	Kesinlik	F1 Ölçütü
%10	90	100	90	94,74
%20	80	100	80	88,89
%30	70	100	70	82,35
%40	60,89	100	60,54	75,42

4.2.2.6. Yapay sinir ağları

Yapay sinir ağları, insan beyninin biyolojik yapısından esinlenerek beyinde bulunan sinir ağı ve nöronların çalışma düzeninin taklit edilmesiyle oluşturulmuş bir modeldir. Tıpkı insan beyninde olduğu gibi yapay sinir ağları da sinir hücrelerinin (nöronlar) birbirine bağlanmasıyla oluşturulmuştur. Nöronların her biri kendisine verilen girdiyi alır, işler ve elde ettiği sonucu diğer nörona aktarır. Bu işlem, birbirine bağlı nöronlarca devam ettirilir. Böylelikle yapay bir sinir ağı oluşturulmuş olur [102, 103]. Şekil 4.3.'de yapay sinir ağlarının katmanlı yapısı gösterilmektedir. Genellikle bu üç katmandan oluşabileceği gibi sistemin yapısına ve beklenen çıktıya göre birden fazla gizli katman da içerebilir.



Şekil 4.3. Yapay sinir ağı modeli.

Giriş katmanı, verilerin yapay sinir ağı modeline girdiği katmandır. Burada veriler, ağ modelindeki hesaplamalar için hazırlanarak gizli katmana iletilir.

Gizli katman, girdi katmanından gelen verileri alır, işler ve veriler arasındaki desenleri tanımlamak için hesaplamalar yapar. Bu hesaplamaya aktivasyon fonksiyonu denir ve yapay sinir ağında bulunan bütün nöronlarda uygulanan matematiksel bir fonksiyondur. Temel amacı, nöronun girdilerine göre aktivasyon seviyesini hesaplamaktır. Nöronun çıktı değeri ise hesaplanan bu seviyeye göre bir eşik değer ile kıyaslanarak belirlenmektedir. Bu çalışma yapısı, ağın derinliğinin artmasına ve daha karmaşık desenleri/problemleri çözebilmesini sağlar. Bir yapay sinir ağı modeli birden fazla gizli katman içerebildiği gibi her katmanda birden fazla nöron olabilir.

Çıkış katmanı, gizli katmandan gelen veriler üzerinde hesaplamalar yaparak yapay sinir ağının çıktılarını üretir. Tasarlanan modele ve ihtiyaçlara göre katmanın yapısı değişiklik gösterir. Örneğin, sınıflandırma için kullanılan modellerde genellikle her biri başka bir sınıfı temsil eden birden fazla çıkış nöronu kullanılırken, regresyon problemlerinde çıkış katmanında tek bir nöron kullanılabilir.

Veriler, belirtilen bu katmanlar arasında girişten çıkışa doğru ilerler ve böylelikle verilerin değerlendirilmesi, işlenmesi ve gereken hesaplamaların yapılması sağlanır. Yapay sinir ağlarının temelini oluşturan bu katmanlar, problemin karmaşıklık düzeyine ve istenen sonuca göre farklı sayıda, boyutta ve yapıda olabilir [104].

Bu tez çalışmasında, yapay sinir ağı modeli RapidMiner programı ile veri setlerine uygulanmıştır. Uygulama sonucunda oluşan modelin sınıflandırma başarım değerleri Tablo 4.8.'deki gibidir.

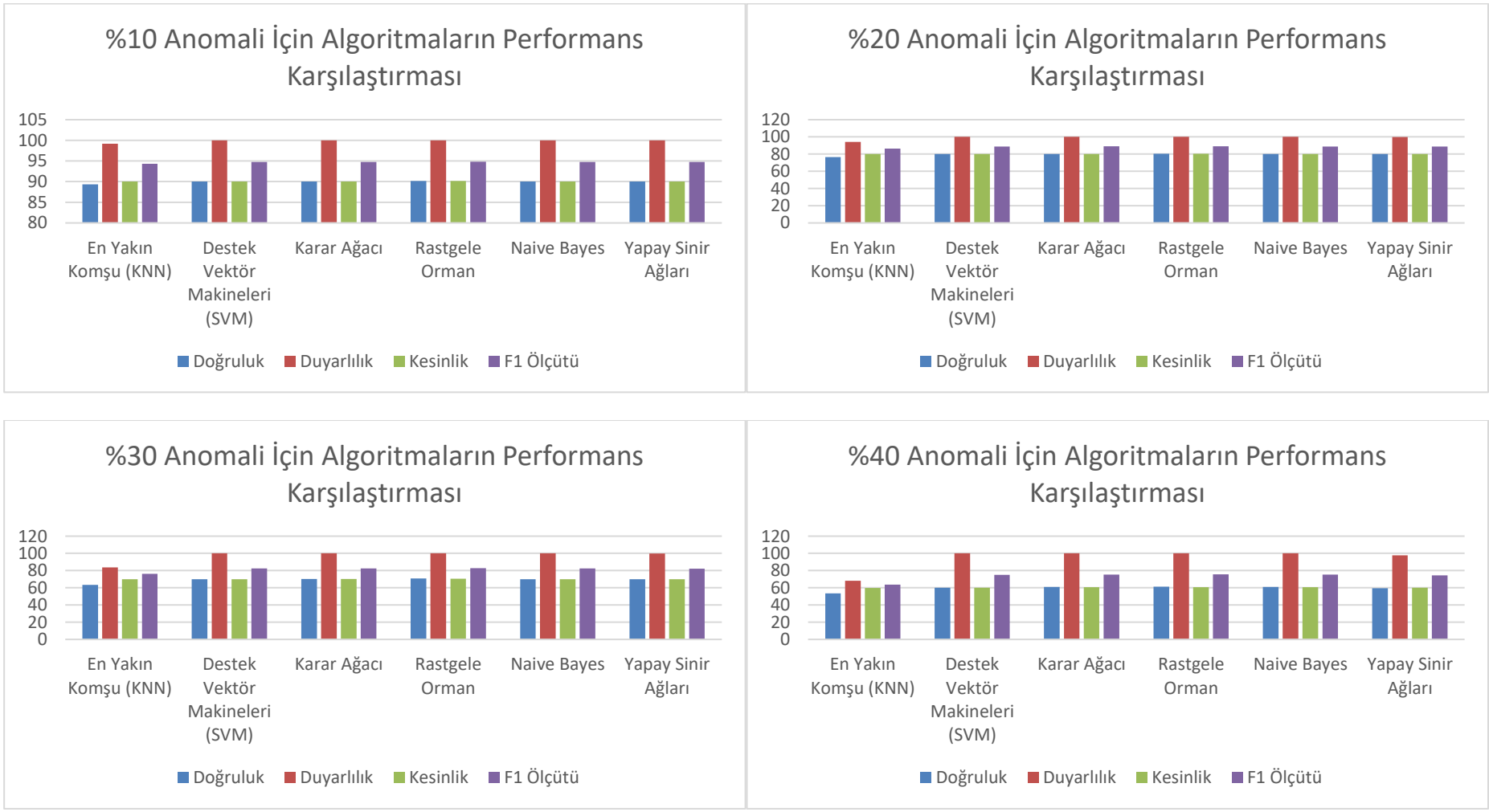
Tablo 4.8. Yapay sinir ağları için test sonuçları.

Anomali Oranı	Doğruluk	Duyarlılık	Kesinlik	F1 Ölçütü
%10	90	100	90	94,74
%20	79,98	99,97	80	88,88
%30	69,9	99,77	70	82,27
%40	59,58	97,85	60,01	74,39

4.3. Algoritmaların Karşılaştırmalı Performans Analizi

Bu tez çalışmasında, akıllı evlerde enerji tüketimine dair oluşturulan veri setlerine k en yakın komşu, destek vektör makineleri, karar ağaçları, rastgele ormanlar, naïve bayes ve yapay sinir ağları makine öğrenme yöntemleri uygulanmış olup, doğruluk, duyarlılık, kesinlik ve f1 ölçütü başarım kriterlerine göre performansları incelenmiştir.

Çalışmanın bu bölümünde, bu tezin bir diğer çıktısı niteliğinde, makine öğrenme algoritmalarının karşılaştırmalı performans analizi yapılacaktır. Simülasyon ortamında modellenen IoT temelli akıllı ev sisteminin enerji tüketim değerleri analiz edilerek algoritmalarca normal veya anormal olarak sınıflandırılmıştır. Bu sınıflandırma işleminin algoritmalarca başarım durumlarındaki performans karşılaştırması, belirlenen başarım metrikleri kapsamında Şekil 4.4.'te sunulmuştur. Doğruluk, duyarlılık, kesinlik ve f1 ölçütü kriterlerine göre yapılan başarım karşılaştırmasında, önerilen modelde kullanılan makine öğrenme algoritmaları farklı anomali değerleri kapsamında incelenmiştir. Bu incelemede, en yakın komşu algoritmasının diğer algoritmalardan daha düşük performans sergilediği görülmektedir. Bununla birlikte, veri setindeki anomali oranının algoritmaların performansına etkisi değerlendirildiğinde, anomali oranındaki artışın algoritmaların performansına ters yönde etki ettiği açıkça görülmektedir. En yakın komşu algoritması haricindeki diğer beş algoritmanın, farklı anomali oranlarında da birbirine yakın sonuçlar verdiği görülmüştür. Nihai olarak tüm algoritmalar karşılaştırıldığında, rastgele orman algoritmasının diğer algoritmalardan daha iyi bir performans gösterdiği anlaşılmaktadır.



Şekil 4.4. Algoritmaların performans karşılaştırması.

5. TARTIŞMA VE SONUÇ

5.1. Sonuçlar

Günümüzdeki enerji şebekelerindeki yetersizlikler akıllı şebeke sistemlerinin kullanılmasını yaygınlaştırmıştır. Gerçek zamanlı veri toplama, analiz etme ve işleme yetenekleri sayesinde akıllı şebekeler, elektrik şebekelerinin verimli bir şekilde yönetilmesine imkan sağlar. Enerji arz ve talebinin yönetilmesi ve izlenmesiyle enerji kaynaklarının daha verimli kullanılmasını sağlasa da birçok farklı cihaz ve protokol barındıran heterojen yapısı sebebiyle karmaşık bir ağ yapısına sahiptir. Bu dezavantajı sebebiyle ortaya çıkan esneklik, ölçeklenebilirlik, programlanabilirlik ve güvenlik gibi sorunların çözümü olarak yazılım tanımlı ağ paradigması önerilmektedir. Ağ cihazlarının merkezi bir sistemle yönetimini sağlayan yapısı sayesinde performansın ve güvenliğin artırılabilmesi bu tercihin ana sebebidir. Öte yandan günümüzde tüketim domaini içerisinde yaygınlaşan IoT temelli cihazların bu sistemlerle entegre şekilde çalışmasıyla kaynakların izlenebilirliği ve enerji tüketim verimliliği artırılabilmektedir. Tüm bu sebeplerden dolayı bu tez çalışmasında, nesnelerin interneti temelli akıllı şebeke sistemleri için yazılım tanımlı bir mimari model önerilmiştir.

Yapılan bu tez çalışmasının ilk aşamasında önerilen, yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı şebeke mimarisi kapsamında günümüzdekine benzer şekilde bir akıllı evde kullanılan IoT destekli cihazların altyapısı modellenmiştir. Modelin simülasyon ortamında çalıştırılabilmesi için sektör ve literatürdeki çalışmalar kapsamlı şekilde incelenmiş ve her bir akıllı cihaz için enerji tüketimini etkileyen faktörler ve tüketim değerleri tespit edilmiştir. Elde edilen parametreler ışığında simülasyon ortamındaki modeli gerçeğe yakın şekilde çalıştıran bir yazılım geliştirilmiştir. Bu yazılım genelde, cihazların enerji tüketimini taklit ederken özelde ise her bir akıllı cihazın çalışmasını ve enerji tüketimini etkileyen başlıca özelliklerini (enerji sınıfı, hacim, program vb.) de taklit eder yapıda geliştirilmiştir.

Tezin ikinci aşamasında, akıllı ev sisteminin çalışması için günümüzdeki akıllı ev yapıları ve kullanıcı profilleri dikkate alınarak kapsamlı çalışma senaryoları

belirlenmiştir. Simülatör ortamındaki model, bu senaryolar kapsamında çalıştırılarak sistem ve tüketim verileri toplanmıştır. Toplanan veriler uygun formata getirilerek, bu tez çalışmasının bir çıktısı olan veri seti oluşturulmuştur. Bu aşamada, daha önce yapılan çalışmalar dikkate alınarak oluşturulan veri setinin literatüre katkı sağlaması hedeflenmiştir. Çalışmanın siber güvenlik alanında da katkı sağlayabilmesi amacıyla verilerin normal-anormal etiketlenmesi gerçekleştirilmiştir. Anormal veriler, literatürdeki akıllı ev sistemlerine gerçekleştirilen siber saldırılar kapsamında manipüle edilerek oluşturulmuştur.

Tezin üçüncü aşamasında, oluşturulan veri setlerinin değerlendirilmesi için makine öğrenme algoritmaları kullanılarak performans karşılaştırması yapılmıştır. Kullanılacak algoritmalar seçilirken veri setine uyumluluğunun yanı sıra kıyas yapılabilmesi açısından literatürdeki diğer çalışmalarda tercih edilmiş olmasına da dikkat edilmiştir. Bununla birlikte, daha etkin bir karşılaştırmanın yapılabilmesi için veri setinde %10, %20, %30 ve %40'lık farklı anomali değerleri oluşturulmuş ve algoritmalar bu kapsamda incelenmiştir. Bu incelemede, en yakın komşu algoritmasının diğer algoritmalardan daha düşük performans sergilediği görülmektedir. Bununla birlikte, veri setindeki anomali oranının algoritmaların performansına etkisi değerlendirildiğinde, anomali oranındaki artışın algoritmaların performansına ters yönde etki ettiği açıkça görülmektedir. En yakın komşu algoritması haricindeki diğer beş algoritmanın, farklı anomali oranlarında da birbirine yakın sonuçlar verdiği görülmüştür. Sonuç olarak, Şekil 4.4.'de verilen performans karşılaştırmasında da görüldüğü üzere, rastgele orman algoritmasının diğer algoritmalardan daha iyi bir performans gösterdiği anlaşılmaktadır.

5.2. Çalışmanın Bilime Katkısı

Bu tez çalışması kapsamında önerilen yazılım tanımlı ağlar ve nesnelerin interneti temelli akıllı şebeke modelinin ve bu modelin bir çıktısı olan veri setlerine uygulanan makine öğrenme algoritmalarının performans karşılaştırmasının literatüre ve bilime katkıları genel olarak şöyle özetlenebilir:

İncelenen akademik çalışmalarda, SDN ve IoT teknolojilerinin akıllı şebekelerdeki tüketim domaini içerisindeki HAN'larda kullanımına rastlanmamıştır. Bu sebeple, bu çalışmada günümüz enerji şebekelerinin ihtiyaçları göz önüne alınarak performans, esneklik, programlanabilirlik ve enerji verimliliği gibi konularda iyileştirme

sağlayacak bir model önerilmiştir. Önerilen bu model, ileride enerji sistemleri üzerine yapılacak çalışmalar için önemli bir birikim sağlayacaktır.

Literatürdeki veri setleri incelendiğinde, akıllı evlerin enerji tüketim verileri ile ilgili bu denli kapsamlı bir çalışmaya rastlanmamıştır. Gerek cihazların özelliklerinin gerekse enerji tüketim değerlerinin gerçek hayattakine yakınlığı sebebiyle özellikle ülkemizdeki akıllı ev sistemleri ele alındığında özgün bir değer ortaya konulduğu söylenebilir. Ayrıca oluşturulan bu veri setlerinin literatüre de büyük katkı sağlayarak bu konuda çalışacak araştırmacılara fayda sağlayacağı öngörülmektedir.

Akıllı ev sistemlerinde veri güvenliği söz konusu olduğunda kullanılacak yöntemler/algoritmalar ile ilgili literatüre katkı sağlaması açısından bu tez çalışmasının bir çıktısı olan veri setleri üzerinde makine öğrenme algoritmalarının performans karşılaştırması gerçekleştirilmiştir. Bu karşılaştırma gerçek veriler üzerinden yapıldığından, akıllı evlerde kullanılacak izleme ve saldırı tespit sistemlerinin geliştirilme sürecine önemli bir yol haritası çizdiği söylenebilir.

5.3. İleriki Çalışmalar

Günümüz enerji sistemlerinin sahip olduğu yetersizlikler büyük bir sorun olarak kalmaya devam edecektir. Dünyada, bu sistemlerin geliştirilmesi için akıllı şebekeler ve yazılım tanımlı ağlar ile entegrasyonunda çeşitli adımlar atılmış olsa da hala daha günümüz ihtiyaçlarını karşılayabilecek seviyeye gelememiştir. Bu kapsamda, bu tez çalışmasında önerilen mimari yapı ve elde edilen bilgi birikimi sonucunda, ileriki çalışma olarak akıllı ev sisteminin raspberry pi ve nodemcu gibi IoT cihazları ile donanımsal olarak da gerçekleştirilmesi hedeflenmektedir. Ayrıca önerilen mimari yapının, yazılım tanımlı ağ yapısında da detaylı çalışmalar yapılarak mimariye daha uygun hale getirilmesi hedeflenmektedir.

Bir başka hedeflenen ileriki çalışma ise, özellikle akıllı evlerdeki enerji tüketimini daha iyi yansıtabilmek amacıyla oluşturulmuş veri setinin geliştirilmesidir. Bu kapsamda, gelişen teknolojiyle birlikte akıllı ev sistemlerinde kullanılmaya başlanan yeni cihazların ve sensörlerin de mimariye eklenerek veri setinde yer alması planlanmaktadır. Bununla birlikte veri setlerinde oluşturulan saldırılara yönelik anomalilerin manipülasyonla değil de doğrudan donanımlara gerçekleştirilmesi neticesinde elde edilmesi hedeflenmektedir. Böylelikle literatüre sunulacak veri setinin gerçek hayata yaklaştırılması hususunda iyileştirilmesi sağlanacaktır.

Akıllı ev sistemlerinde önemli olan bir diğer konu ise bu sistemlerin altyapılarının güvenliğidir. Bu kapsamda diğer bir çalışma olarak hem IoT cihazları üzerinde hem de iletim altyapısında yaşanabilecek siber saldırılara karşı ağ içindeki anomalileri tespit edebilecek bir uygulama geliştirilmesi planlanmaktadır. Bu sistemle birlikte akıllı ev sisteminin izlenebilirliğini artıracak bir arayüz de oluşturulacaktır.

KAYNAKLAR

[1] Rehmani, M. H., Davy, A., Jennings, B., & Assi, C. (2019). Software defined networks-based smart grid communication: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(3), 2637-2670. https://doi.org/10.1109/COMST.2019.2908266

[2] Demirci, S., & Sagiroglu, S. (2018, October). Software-defined networking for improving security in smart grid systems. In 2018 7th International Conference on Renewable Energy Research and Applications (ICRERA) (pp. 1021-1026). IEEE. https://doi.org/10.1109/ICRERA.2018.8567005

[3] Soares, A. A., Lopes, Y., Passos, D., Fernandes, N. C., & Muchaluat-Saade, D. C. (2021). 3AS: Authentication, authorization, and accountability for sdn-based smart grids. IEEE Access, 9, 88621-88640. https://doi.org/10.1109/ACCESS.2021.3090346

[4] Dorsch, N., Kurtz, F., & Wietfeld, C. (2017, November). Communications in distributed smart grid control: Software-defined vs. legacy networks. In 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2) (pp. 1-6). IEEE. https://doi.org/10.1109/EI2.2017.8245292

[5] Özçelik, İ., İskefiyeli, M., Balta, M., Akpinar, K. O., & Toker, F. S. (2021, December). Center energy: A secure testbed infrastructure proposal for electricity power grid. In 2021 International Conference on Information Security and Cryptology (ISCTURKEY) (pp. 149-154). IEEE. https://doi.org/10.1109/ISCTURKEY53027.2021.9654352

[6] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51. https://doi.org/10.1109/MSP.2011.67

[7] Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1-29.

[8] Tuballa, M. L., & Abundo, M. L. (2016). A review of the development of Smart Grid technologies. Renewable and Sustainable Energy Reviews, 59, 710-725. https://doi.org/10.1016/j.rser.2016.01.011

[9] Sioshansi, F. (Ed.). (2011). Smart grid: integrating renewable, distributed and efficient energy. Academic Press.

[10] Farhangi, H. (2009). The path of the smart grid. IEEE power and energy magazine, 8(1), 18-28. https://doi.org/10.1109/MPE.2009.934876

[11] Gilbert, G. M., Naiman, S., Kimaro, H., & Bagile, B. (2019). A critical review of edge and fog computing for smart grid applications. In Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D: 15th IFIP WG 9.4 International Conference on Social Implications of Computers in Developing Countries, ICT4D 2019, Dar es Salaam, Tanzania, May 1–3, 2019, Proceedings, Part I 15 (pp. 763-775). Springer International Publishing. https://doi.org/10.1007/978-3-030-18400-1_62

[12] Kabalci, Y., Kabalci, E., Padmanaban, S., Holm-Nielsen, J. B., & Blaabjerg, F. (2019). Internet of things applications as energy internet in smart grids and smart environments. Electronics, 8(9), 972. https://doi.org/10.3390/electronics8090972

[13] Avancini, D. B., Rodrigues, J. J., Martins, S. G., Rabêlo, R. A., Al-Muhtadi, J., & Solic, P. (2019). Energy meters evolution in smart grids: A review. Journal of cleaner production, 217, 702-715. https://doi.org/10.1016/j.jclepro.2019.01.229

[14] Dileep, G. (2020). A survey on smart grid technologies and applications. Renewable energy, 146, 2589-2625. https://doi.org/10.1016/j.renene.2019.08.092

[15] Abrahamsen, F. E., Ai, Y., & Cheffena, M. (2021). Communication technologies for smart grid: A comprehensive survey. Sensors, 21(23), 8087. https://doi.org/10.3390/s21238087

[16] Mohammed, A., & George, G. (2022, March). Vulnerabilities and strategies of cybersecurity in smart grid-evaluation and review. In 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE) (pp. 1-6). IEEE. https://doi.org/10.1109/SGRE53517.2022.9774038

[17] Ortega-Fernandez, I., & Liberati, F. (2023). A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. Energies, 16(2), 635. https://doi.org/10.3390/en16020635

[18] NIST (2018, 8 Kasım). Update of the NIST Smart Grid Conceptual Model. https://www.nist.gov/system/files/documents/2018/11/08/draft_smart_grid_conceptual_model_update_v3.pdf adresinden 2 Nisan 2023 tarihinde alınmıştır.

[19] CEN-CENELEC-ETSI Smart Grid Coordination Group (2012, Kasım). Smart Grid Reference Architecture. https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/reference_architecture_smartgrids.pdf adresinden 2 Nisan 2023 tarihinde alınmıştır.

[20] Akyildiz, I. F., Lee, A., Wang, P., Luo, M., & Chou, W. (2014). A roadmap for traffic engineering in SDN-OpenFlow networks. Computer Networks, 71, 1-30. https://doi.org/10.1016/j.comnet.2014.06.002

[21] Singh, A. K., & Srivastava, S. (2018). A survey and classification of controller placement problem in SDN. International Journal of Network Management, 28(3), e2018. https://doi.org/10.1002/nem.2018

[22] Ujjan, R. M. A., Pervez, Z., Dahal, K., Khan, W. A., Khattak, A. M., & Hayat, B. (2021). Entropy based features distribution for anti-ddos model in sdn. Sustainability, 13(3), 1522. https://doi.org/10.3390/su13031522

[23] Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials, 18(1), 602-622. https://doi.org/10.1109/COMST.2015.2487361

[24] Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013, November). SDN security: A survey. In 2013 IEEE SDN For Future Networks and Services (SDN4FNS) (pp. 1-7). IEEE. https://doi.org/10.1109/SDN4FNS.2013.6702553

[25] Farhady, H., Lee, H., & Nakao, A. (2015). Software-defined networking: A survey. Computer Networks, 81, 79-95. https://doi.org/10.1016/j.comnet.2015.02.014

[26] Rawat, D. B., & Reddy, S. R. (2016). Software defined networking architecture, security and energy efficiency: A survey. IEEE Communications Surveys & Tutorials, 19(1), 325-346. https://doi.org/10.1109/COMST.2016.2618874

[27] Paliwal, M., Shrimankar, D., & Tembhurne, O. (2018). Controllers in SDN: A review report. IEEE access, 6, 36256-36270. https://doi.org/10.1109/ACCESS.2018.2846236

[28] Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1761-1804. https://doi.org/10.1109/COMST.2020.2997475

[29] Chica, J. C. C., Imbachi, J. C., & Vega, J. F. B. (2020). Security in SDN: A comprehensive survey. Journal of Network and Computer Applications, 159, 102595. https://doi.org/10.1016/j.jnca.2020.102595

[30] Alabbad, M., & Khedri, R. (2021). Configuration and governance of dynamic secure SDN. Procedia Computer Science, 184, 131-139. https://doi.org/10.1016/j.procs.2021.03.024

[31] Hussain, M., Shah, N., Amin, R., Alshamrani, S. S., Alotaibi, A., & Raza, S. M. (2022). Software-defined networking: Categories, analysis, and future directions. Sensors, 22(15), 5551. https://doi.org/10.3390/s22155551

[32] Sharma, A., Balasubramanian, V., & Kamruzzaman, J. (2023). A Novel Dynamic Software-Defined Networking Approach to Neutralize Traffic Burst. Computers, 12(7), 131. https://doi.org/10.3390/computers12070131

[33] Schaller, S., & Hood, D. (2017). Software defined networking architecture standardization. Computer standards & interfaces, 54, 197-202 https://doi.org/10.1016/j.csi.2017.01.005

[34] Rawat, D. B., & Reddy, S. R. (2016). Software defined networking architecture, security and energy efficiency: A survey. IEEE Communications Surveys & Tutorials, 19(1), 325-346. https://doi.org/10.1109/COMST.2016.2618874

[35] Balta, M. (2019). Şehir içi trafik yönetim sistemleri için sdn temelli bir vanet mimari önerisi ve sinyalizasyon uygulaması [Doktora Tezi] Sakarya Üniversitesi https://doi.org/10.17341/gazimmfd.460544

[36] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2018). A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable cities and society, 38, 806-835. https://doi.org/10.1016/j.scs.2017.12.041

[37] Sedaghati, R., & Shakarami, M. R. (2019). A novel control strategy and power management of hybrid PV/FC/SC/battery renewable power system-based grid-connected microgrid. Sustainable Cities and Society, 44, 830-843. https://doi.org/10.1016/j.scs.2018.11.014

[38] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 944–980, Oct. 2012. https://doi.org/10.1109/SURV.2011.101911.00087

[39] Kafle, Y. R., Mahmud, K., Morsalin, S., & Town, G. E. (2016, September). Towards an internet of energy. In 2016 IEEE International Conference on Power System Technology (POWERCON) (pp. 1-6). IEEE. https://doi.org/10.1109/POWERCON.2016.7754036

[40] Abujubbeh, M., Al-Turjman, F., & Fahrioglu, M. (2019). Software-defined wireless sensor networks in smart grids: An overview. Sustainable Cities and Society, 51, 101754. https://doi.org/10.1016/j.scs.2019.101754

[41] B. Kroposki et al., "Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable energy," IEEE Power Energy Mag., vol. 15, no. 2, pp. 61–73, Mar./Apr. 2017 https://doi.org/10.1109/MPE.2016.2637122

[42] A. Zipperer et al., "Electric energy management in the smart home: Perspectives on enabling technologies and consumer behavior," Proc. IEEE, vol. 101, no. 11, pp. 2397–2408, Nov. 2013. https://doi.org/10.1109/JPROC.2013.2270172

[43] A. Sydney, J. Nutaro, C. Scoglio, D. Gruenbacher, and N. Schulz, "Simulative comparison of multiprotocol label switching and OpenFlow network technologies for transmission operations," IEEE Trans. Smart Grid, vol. 4, no. 2, pp. 763–770, Jun. 2013. https://doi.org/10.1109/TSG.2012.2227516

[44] N. Dorsch, F. Kurtz, H. Georg, C. Hagerling, and C. Wietfeld, "Software-defined networking for smart grid communications: Applications, challenges and advantages," in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Nov. 2014, pp. 422–427. https://doi.org/10.1109/SmartGridComm.2014.7007683

[45] Y.-J. Kim, K. He, M. Thottan, and J. G. Deshpande, "Virtualized and self-configurable utility communications enabled by software-defined networks," in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Nov. 2014, pp. 416–421. https://doi.org/10.1109/SmartGridComm.2014.7007682

[46] N. Dorsch et al., “Intertwined: Software-defined communication networks for multi-agent system-based smart grid control,” in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Nov. 2016, pp. 254–259. https://doi.org/10.1109/SmartGridComm.2016.7778770

[47] M. Donohoe, B. Jennings, and S. Balasubramaniam, “Contextawareness and the smart grid: Requirements and challenges,” Comput. Netw., vol. 79, pp. 263–282, Mar. 2015. https://doi.org/10.1016/j.comnet.2015.01.007

[48] F. Bannour, S. Souihi, and A. Mellouk, “Distributed SDN control: Survey, taxonomy and challenges,” IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 333–354, 1st Quart., 2018. https://doi.org/10.1109/COMST.2017.2782482

[49] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, “In-band control, queuing, and failure recovery functionalities for OpenFlow,” IEEE Netw., vol. 30, no. 1, pp. 106–112, Jan./Feb. 2016. https://doi.org/10.1109/MNET.2016.7389839

[50] Dong, X., Lin, H., Tan, R., Iyer, R. K., & Kalbarczyk, Z. (2015, April). Software-defined networking for smart grid resilience: Opportunities and challenges. In Proceedings of the 1st ACM workshop on cyber-physical system security (pp. 61-68). https://doi.org/10.1145/2732198.2732203

[51] Chekired, D. A., Khoukhi, L., & Mouftah, H. T. (2017). Decentralized cloud-SDN architecture in smart grid: A dynamic pricing model. IEEE Transactions on Industrial Informatics, 14(3), 1220-1231. https://doi.org/10.1109/TII.2017.2742147

[52] Al-Rubaye, S., Kadhum, E., Ni, Q., & Anpalagan, A. (2017). Industrial internet of things driven by SDN platform for smart grid resiliency. IEEE Internet of Things Journal, 6(1), 267-277. https://doi.org/10.1109/JIOT.2017.2734903

[53] Li, J., Cai, J., Khan, F., Rehman, A. U., Balasubramaniam, V., Sun, J., & Venu, P. (2020). A secured framework for sdn-based edge computing in IOT-enabled healthcare system. IEEE Access, 8, 135479-135490. https://doi.org/10.1109/ACCESS.2020.3011503

[54] Li, X., Zhou, C., Liang, Z., Yu, Q., Chen, X., & He, Z. (2022). UCB-Based Route and Power Selection Optimization for SDN-Enabled Industrial IoT in Smart Grid. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/7424854

[55] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[56] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1-31. https://doi.org/10.1016/j.comcom.2014.09.008

[57] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[58] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

[59] Aazam, M., Zeadally, S., & Harras, K. A. (2020). Health fog for smart healthcare. IEEE Consumer Electronics Magazine, 9(2), 96-102. https://doi.org/10.1109/MCE.2019.2953749

[60] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European research projects on the internet of things, European Commision, 3(3), 34-36.

[61] Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. Computer, 44(9), 51-58. https://doi.org/10.1109/MC.2011.291

[62] El-Sayed, H., Sankar, S., Prasad, M., Puthal, D., Gupta, A., Mohanty, M., & Lin, C. T. (2017). Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment. ieee access, 6, 1706-1717. https://doi.org/10.1109/ACCESS.2017.2780087

[63] Hakim, A., Amirat, A., & Oussalah, M. C. (2020). Non-intrusive contextual dynamic reconfiguration of ambient intelligent IoT systems. Journal of Ambient Intelligence and Humanized Computing, 11(4), 1365-1376. https://doi.org/10.1007/s12652-018-1127-2

[64] Özdoğan, E., & Resul, D. A. Ş. (2021). IoT based a Smart Home Automation System Design: Simulation Case. Balkan Journal of Electrical and Computer Engineering, 9(3), 297-303. https://doi.org/10.17694/bajece.918826

[65] Rondon, L. P., Babun, L., Aris, A., Akkaya, K., & Uluagac, A. S. (2022). Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. Ad Hoc Networks, 125, 102728. https://doi.org/10.1016/j.adhoc.2021.102728

[66] Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1, 81-98. https://doi.org/10.1016/j.iot.2018.08.009

[67] Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. sensors, 18(3), 817. https://doi.org/10.3390/s18030817

[68] Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change, 138, 139-154. https://doi.org/10.1016/j.techfore.2018.08.015

[69] Zaidan, A. A., & Zaidan, B. B. (2020). A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artificial Intelligence Review, 53(1), 141-165. https://doi.org/10.1007/s10462-018-9648-9

[70] Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. Sensors, 21(11), 3784. https://doi.org/10.3390/s21113784

[71] Darem, A., Alhashmi, A. A., & Jemal, H. A. (2022). Cybersecurity Threats and Countermeasures of the Smart Home Ecosystem. IJCSNS, 22(3), 303. https://doi.org/10.22937/IJCSNS.2022.22.3.39

[72] E. D. L. Oliveira, R. D. Alfaia, A. V. F. Souto, M. S. Silva, C. R. L. Francás, and N. L. Vijaykumar, ‘‘SmartCoM: Smart consumption management architecture for providing a user- friendly smart home based on metering and computational intelligence,’’ J. Microw., Optoelectron. Electromagn. Appl., vol. 16, no. 3, pp. 736–755, Sep. 2017. https://doi.org/10.1590/2179-10742017v16i3965

[73] Mininet Overview. http://mininet.org/ adresinden 8 Nisan 2023 tarihinde alınmıştır. http://mininet.org/overview/

[74] Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I., & Ahmed, A. (2019). Edge computing: A survey. Future Generation Computer Systems, 97, 219-235. https://doi.org/10.1016/j.future.2019.02.050

[75] Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An overview on edge computing research. IEEE access, 8, 85714-85728. https://doi.org/10.1109/ACCESS.2020.2991734

[76] Darroudi, S. M., & Gomez, C. (2017). Bluetooth low energy mesh networks: A survey. Sensors, 17(7), 1467. https://doi.org/10.3390/s17071467

[77] Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 7(3), 28. https://doi.org/10.3390/jsan7030028

[78] Danbatta, S. J., & Varol, A. (2019, June). Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE. https://doi.org/10.1109/ISDFS.2019.8757472

[79] Çorak, B. H., Okay, F. Y., Güzel, M., Murt, Ş., & Ozdemir, S. (2018, June). Comparative analysis of IoT communication protocols. In 2018 International symposium on networks, computers and communications (ISNCC) (pp. 1-6). IEEE. https://doi.org/10.1109/ISNCC.2018.8530963

[80] Al Enany, M. O., Harb, H. M., & Attiya, G. (2021, July). A Comparative analysis of MQTT and IoT application protocols. In 2021 International Conference on Electronic Engineering (ICEEM) (pp. 1-6). IEEE. https://doi.org/10.1109/ICEEM52022.2021.9480384

[81] Wang, Y., Chen, C., & Jiang, Q. (2019). Security algorithm of Internet of Things based on ZigBee protocol. Cluster Computing, 22, 14759-14766. https://doi.org/10.1007/s10586-018-2388-4

[82] Haque, H., Labeeb, K., Riha, R. B., & Khan, M. N. R. (2021, March). IoT based water quality monitoring system by using Zigbee protocol. In 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 619-622). IEEE. https://doi.org/10.1109/ESCI50559.2021.9397031

[83] de Oliveira, K. V., Castelli, H. M. E., Montebeller, S. J., & Avancini, T. G. P. (2017, August). Wireless sensor network for smart agriculture using ZigBee protocol. In 2017 IEEE First Summer School on Smart Cities (S3C) (pp. 61-66). IEEE. https://doi.org/10.1109/S3C.2017.8501379

[84] Pahlavan, K., & Krishnamurthy, P. (2021). Evolution and impact of Wi-Fi technology and applications: A historical perspective. International Journal of Wireless Information Networks, 28, 3-19. https://doi.org/10.1007/s10776-020-00501-8

[85] Fan, C., Chen, M., Wang, X., Wang, J., & Huang, B. (2021). A review on data preprocessing techniques toward efficient and reliable knowledge discovery from building operational data. Frontiers in Energy Research, 9, 652801. https://doi.org/10.3389/fenrg.2021.652801

[86] Yu, X., Ergan, S., & Dedemen, G. (2019). A data-driven approach to extract operational signatures of HVAC systems and analyze impact on electricity consumption. Applied Energy, 253, 113497. https://doi.org/10.1016/j.apenergy.2019.113497

[87] Fan, C., Xiao, F., & Yan, C. (2015). A framework for knowledge discovery in massive building automation data and its application in building diagnostics. Automation in Construction, 50, 81-90. https://doi.org/10.1016/j.autcon.2014.12.006

[88] Fan, C., Xiao, F., Madsen, H., & Wang, D. (2015). Temporal knowledge discovery in big BAS data for building energy management. Energy and Buildings, 109, 75-89. https://doi.org/10.1016/j.enbuild.2015.09.060

[89] Data Never Sleeps 10.0. https://www.domo.com/data-never-sleeps adresinden 9 Mayıs 2023 tarihinde alınmıştır.

[90] Gangwar, A. K., & Shaik, A. G. (2023). k-Nearest neighbour based approach for the protection of distribution network with renewable energy integration. *Electric Power Systems Research*, *220*, 109301 https://doi.org/10.1016/j.epsr.2023.109301

[91] Widodo, A., & Yang, B. S. (2007). Support vector machine in machine condition monitoring and fault diagnosis. Mechanical systems and signal processing, 21(6), 2560-2574. https://doi.org/10.1016/j.ymssp.2006.12.007

[92] Liu, R., Yang, B., Zio, E., & Chen, X. (2018). Artificial intelligence for fault diagnosis of rotating machinery: A review. Mechanical Systems and Signal Processing, 108, 33-47. https://doi.org/10.1016/j.ymssp.2018.02.016

[93] Ray, S. (2019, February). A quick review of machine learning algorithms. In 2019 International conference on machine learning, big data, cloud and parallel computing (COMITCon) (pp. 35-39). IEEE. https://doi.org/10.1109/COMITCon.2019.8862451

[94] Charbuty, B., & Abdulazeez, A. (2021). Classification based on decision tree algorithm for machine learning. Journal of Applied Science and Technology Trends, 2(01), 20-28.

[95] Kamiński, B., Jakubczyk, M., & Szufel, P. (2018). A framework for sensitivity analysis of decision trees. Central European journal of operations research, 26, 135-159. https://doi.org/10.1007/s10100-017-0479-6

[96] Hasan, M. A. M., Nasser, M., Ahmad, S., & Molla, K. I. (2016). Feature selection for intrusion detection using random forest. Journal of information security, 7(3), 129-140. http://dx.doi.org/10.4236/jis.2016.73009

[97] Duggal, P., & Shukla, S. (2020, January). Prediction of thyroid disorders using advanced machine learning techniques. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 670-675). IEEE. https://doi.org/10.1109/Confluence47617.2020.9058102

[98] Berrar, D. (2018). Bayes' theorem and naive Bayes classifier. Encyclopedia of Bioinformatics and Computational Biology: ABC of Bioinformatics, 403, 412.

[99] Alzubi, J., Nayyar, A., & Kumar, A. (2018, November). Machine learning from theory to algorithms: an overview. In Journal of physics: conference series (Vol. 1142, p. 012012). IOP Publishing. http://dx.doi.org/10.1088/1742-6596/1142/1/012012

[100] Vadivukarassi, M., Puviarasan, N., & Aruna, P. (2017). Sentimental analysis of tweets using Naive Bayes algorithm. World Applied Sciences Journal, 35(1), 54-59.

[101] Mahesh, B. (2020). Machine learning algorithms-a review. International Journal of Science and Research (IJSR).[Internet], 9, 381-386. http://dx.doi.org/10.21275/ART20203995

[102] Chen, M., Challita, U., Saad, W., Yin, C., & Debbah, M. (2019). Artificial neural networks-based machine learning for wireless networks: A tutorial. IEEE Communications Surveys & Tutorials, 21(4), 3039-3071. https://doi.org/10.1109/COMST.2019.2926625

[103] Kuo, P. H., & Huang, C. J. (2018). A high precision artificial neural networks model for short-term energy load forecasting. Energies, 11(1), 213. https://doi.org/10.3390/en11010213

[104] Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. Ict Express, 4(2), 95-99. https://doi.org/10.1016/j.icte.2018.04.003

[105] Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In 2015 military communications and information systems conference (MilCIS) (pp. 1-6). IEEE. https://doi.org/10.1109/MilCIS.2015.7348942

[106] Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2017, June). Flow-based benchmark data sets for intrusion detection. In Proceedings of the 16th European conference on cyber warfare and security. ACPI (pp. 361-369).

[107] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108-116. https://doi.org/10.5220/0006639801080116

[108] Moustafa, N. (2019, October). New generations of internet of things datasets for cybersecurity applications based machine learning: TON_IoT datasets. In Proceedings of the eResearch Australasia Conference, Brisbane, Australia (pp. 21-25).

[109] NSL-KDD dataset. https://www.unb.ca/cic/datasets/nsl.html adresinden 4 Mayıs 2023 tarihinde alınmıştır.

EKLER

EK A. Cihaz özellikleri tabloları

EK A

Tablo A.1. Buzdolabı özellik tablosu.

Buzdolabı			
Enerji Sınıfı	Hacim	Evde Yaşayan Kişi Sayısı	Tüketilen Enerji
D	Büyük	1	X
E	Orta	2	
F	Mini	3	
		4	

Tablo A.2. Bulaşık makinesi özellik tablosu.

Bulaşık Makinesi				
Enerji Sınıfı	Su Tüketimi	Program	Haftalık Kullanım Sayısı	Tüketilen Enerji
C	9,5	Yoğun	1	X
D	11,5	Eko	2	
E	12,9	Hızlı	3	
		Ön Yıkama	4	

Tablo A.3. Fırın özellik tablosu.

Fırın				
Enerji Sınıfı	Tür	Program	Haftalık Kullanım Sayısı	Tüketilen Enerji
A	Ankastre Fırın	Kırmızı Et	1	X
B	Ocaklı Fırın	Tavuk	2	
		Balık	3	
		Sebze	4	
		Kek		
		Hamur İşi		

Tablo A.4. Çamaşır makinesi özellik tablosu.

Çamaşır Makinesi					
Enerji Sınıfı	Hacim	Devir	Program	Haftalık Kullanım Sayısı	Tüketilen Enerji
A	8 kg	1000	Pamuklu	1	X
B	9 kg	1200	Sentetik	2	
C	10 kg	1400	Eko	3	
			Hızlı	4	

Tablo A.5. Televizyon özellik tablosu.

Televizyon				
Enerji Sınıfı	Ekran Tipi	Ekran Boyutu	Haftalık Kullanım Süresi	Tüketilen Enerji
E	FHD	50''	1-4 saat	X
F	4K UHD	55''	4-8 saat	
G		65''	8-12 saat	
			12+ saat	

Tablo A.6. Klima özellik tablosu.

Klima				
Enerji Sınıfı	Tür	Kapasite	Haftalık Kullanım Sayısı	Tüketilen Enerji
A	Split	12000 Btu/h	1-4 saat	X
B	Mobil	18000 Btu/h	4-8 saat	
C	Salon Tipi	24000 Btu/h	8-12 saat	
			12+ saat	

Tablo A.7. Aydınlatma özellik tablosu.

Aydınlatma			
Tür	Ampul Sayısı	Haftalık Kullanım Süresi	Tüketilen Enerji
Led	1-6	1-10 saat	X
Floresan	7-12	10-20 saat	
Halojen	13-18	20-30 saat	
	19-24	30+ saat	

Tablo A.8. Küçük ev aletleri özellik tablosu.

Küçük Ev Aletleri			
Tür	Güç	Haftalık Kullanım Süresi	Tüketilen Enerji
Tost Makinesi	Seviye 1	1-4 saat	X
Kettle	Seviye 2	4-7 saat	
Ütü	Seviye 3	7-10 saat	
Süpürge	Seviye 4	10+ saat	

ÖZGEÇMİŞ

Ad-Soyad : Hilal YILDIZ

ÖĞRENİM DURUMU:

- **Lisans :** 2021, Sakarya Üniversitesi, Bilgisayar ve Bilişim Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2022 yılında Sakarya Üniversitesi Bilgisayar ve Bilişim Bilimleri Fakültesi Bilgisayar Mühendisliği bölümünde araştırma görevlisi olarak çalışmaya başladı.

DİĞER ESERLER:

Yıldız, H., & Balta, M. (2022). Web Based Health Check Application for Water Management Systems via SNMP Protocol. Academic Perspective Procedia, 5(3), 328-337.