

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ



BULUT BİLİŞİM SİSTEMLERİNE YAPILAN SALDIRILARIN
DERİN ÖĞRENME YÖNTEMİ İLE ANALİZİ

Tuğba TEKKOL

Yüksek Lisans Tezi

YAZILIM MÜHENDİSLİĞİ ANABİLİM DALI

Ekim 2023

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yazılım Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

BULUT BİLİŞİM SİSTEMLERİNE YAPILAN SALDIRILARIN DERİN ÖĞRENME YÖNTEMİ İLE ANALİZİ

Tez Yazarı
Tuğba TEKKOL

Danışman
Doç. Dr. Muhammet BAYKARA

Ekim 2023
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yazılım Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Bulut Bilişim Sistemlerine Yapılan Saldırıların Derin Öğrenme Yöntemi İle Analizi
Yazarı:	Tuğba TEKKOL
İlk Teslim Tarihi:	10.06.2023
Savunma Tarihi:	11.10.2023

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

Danışman:	Doç. Dr. Muhammet BAYKARA Fırat Üniversitesi, Teknoloji Fakültesi	İmza Onayladım
Başkan:	Prof. Dr. Engin AVCI Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Talha Burak ALAKUŞ Kırklareli Üniversitesi, Mühendislik Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun/...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Burhan ERGEN
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım “Bulut Bilişim Sistemlerine Yapılan Saldırıların Derin Öğrenme Yöntemi İle Analizi” Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

11.10.2023

Tuğba TEKKOL



ÖNSÖZ

Bulut bilişim, veri depolama, erişim kolaylığı, ölçeklenebilirliği, esnek oluşu ve maliyet etkinliği gibi birçok avantaja sahip olması, son yıllarda iş dünyasında ve teknoloji alanında yeni bir devrim yaratmıştır. Bulut bilişimin potansiyel kazanımlarına rağmen, işletmelerin verilerini üçüncü taraflarla paylaşması konusunda bazı endişeler oluşmuştur. Ayrıca, bulut pazarının büyümesi, kötü niyetli kişileri de harekete geçirmiştir. Bu nedenle, bulutun avantajlarından yararlanmadan önce güvenlik konusundaki tereddütlerin giderilmesi önemlidir.

Bu tez çalışmasında, bilgi ve tecrübelerini benimle paylaşan değerli hocam ve danışmanım Doç. Dr. Muhammet BAYKARA' ya çok teşekkür ederim. Ayrıca bu tez çalışması, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından **TEKF.22.24** protokol numaralı proje ile desteklenmiştir.

Tuğba TEKKOL
ELAZIĞ, 2023

İÇİNDEKİLER

Sayfa

ÖNSÖZ.....	iv
İÇİNDEKİLER	v
ÖZET	vii
ABSTRACT	viii
ŞEKİLLER LİSTESİ	ix
TABLolar LİSTESİ	x
SİMGELER VE KISALTMALAR	xi
1. GİRİŞ	1
2. BULUT BİLİŞİM.....	5
2.1. Bulut Dağıtım Modelleri	6
2.2. Bulut Hizmet Modelleri.....	7
2.2.1. Hizmet Olarak Altyapı	7
2.2.2. Hizmet Olarak Platform	8
2.2.3. Hizmet Olarak Yazılım	8
2.3. Bulutta Yaşanan Güvenlik Sorunları	9
2.3.1. Hizmet Olarak Altyapı Modelinde Yaşanan Güvenlik Sorunları	9
2.3.2. Hizmet Olarak Platform Modelinde Yaşanan Güvenlik Sorunları	11
2.3.3. Hizmet Olarak Yazılım Modelinde Yaşanan Güvenlik Sorunları	12
2.3.4. Bulut Hizmetlerinde Güvenlik: HOA, HOP, HOY Farkları.....	13
2.4. Bulutta Yaşanan Güvenlik Sorunlarına Karşı Alınan Önlemler	13
3. DERİN ÖĞRENME	15
3.1. Evrişimsel Sinir Ağları	16
3.2. Tekrarlayıcı Sinir Ağı.....	17
3.2.1. Uzun Kısa Süreli Bellek	18
3.3. Derin Öğrenme Yöntemlerinin Saldırı Tespit Sistemlerinde Kullanılması	18
3.3.1. Anomali Tespiti.....	19
3.3.2. İmza Tabanlı Tespitin Güçlendirilmesi	19
3.3.3. Veri Madenciliği ve Özellik Çıkarımı	20
3.3.4. Gerçek Zamanlı Saldırı Tespiti	20
4. MATERYAL VE METOT	22
4.1. Materyal.....	22
4.2. Metot	23
4.2.1. Softmax Aktivasyon Fonksiyonu	24
4.2.2. Çapraz Doğrulama Yöntemi.....	24
4.2.3. Paralel ESA-UKSB Tabanlı İzinsiz Giriş Modeli	25
4.2.4. Hiyerarşik ESA-UKSB Tabanlı İzinsiz Giriş Tespit Modeli	26
4.3. Performans Değerlendirme	27
5. BULGULAR.....	30
5.1. UNSW-NB15 Veri Seti Kullanılarak Hiyerarşik ve Paralel ESA-UKSB Modelinin Değerlendirilmesi.....	30
5.2. AWID Veri Seti Kullanılarak Hiyerarşik ve Paralel ESA-UKSB Modelinin Değerlendirilmesi ...	35

6. SONUÇLAR VE TARTIŞMA.....	41
ÖNERİLER	43
KAYNAKLAR.....	44
ÖZGEÇMİŞ	



ÖZET

Bulut Bilişim Sistemlerine Yapılan Saldırıların Derin Öğrenme Yöntemi İle Analizi

Tuğba TEKKOL

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Yazılım Mühendisliği Anabilim Dalı

Ekim 2023, Sayfa: xi + 49

Bulut bilişim, sunucular, depolama alanı, ağ altyapısı, veri merkezi ve yazılım hizmetleri gibi bilgi işlem kaynaklarının ortak bir ağ üzerinden sunulduğu bir hizmet modelidir. Bu hizmet modeli, kullanıcılara esneklik, ölçeklenebilirlik ve maliyet tasarrufu sağlamaktadır. Bulut bilişim potansiyel kazanımlarına rağmen güvenlik konusunda sıkıntılar nedeniyle bireyler ve işletmeler tarafından tam benimsenmemektedir. Bu nedenle bulut bilişim güvenliği yeni bir araştırma konusu haline gelmiştir.

Derin öğrenme, bulut bilişim güvenliği alanında önemli bir potansiyele sahiptir. Güvenlik tehditlerinin karmaşıklığı ve hacmi arttıkça, derin öğrenme algoritmaları, bulut sistemlerindeki güvenlik açıklarını tespit etme, saldırıları önleme ve veri gizliliğini sağlama konularında etkili bir rol oynayabilir. Derin öğrenme tabanlı analiz yöntemleri, büyük veri kümelerini inceleyerek anormal davranışları tespit edebilir ve hızlı bir şekilde yanıt verilmesini sağlayabilir. Bu büyük veri incelemeleri genellikle sinir ağı mimarilerini kullanır.

Bu tez çalışmasında, bulut bilişimde ortaya çıkan güvenlik sorunları hakkında kapsamlı bir araştırma yapılmıştır. Bulut bilişimin hizmet olarak altyapı modelinde yaşanan sıkıntılar diğer hizmet modellerini etkilemektedir. Bu nedenle derin öğrenme teknikleri kullanılarak, çeşitli saldırı türlerini ve normal ağ trafiğini temsil eden UNSW-NB15 ve AWID adındaki geniş veri kümeleri kullanılarak ağ davranışları izlenmiştir. Çalışma kapsamında derin öğrenme alanında yaygın olarak kullanılan Evrişimsel Sinir Ağı (ESA) ve Tekrarlayıcı Sinir Ağı (TSA)'nın bir türü olan Uzun-Kısa Süreli Bellek (UKSB) sinir ağlarından iki model oluşturulmuştur. İlk modelde, hiyerarşik bir yapı söz konusu olup UKSB, ESA tarafından öğrenilen giriş verilerinin özelliklerini öğrenmek için kullanılmaktadır. İkinci modelde ise ESA ve UKSB, giriş verileri üzerinde bağımsız olarak çalışmakta ve çıktıları paralel bir şekilde birleştirilmektedir. Bu iki model, yukarıda bahsedilen veri setleriyle eğitilip test edildikten sonra elde edilen sonuçlar karşılaştırılmaktadır. UNSW-NB15 veri seti üzerinde hiyerarşik ESA-UKSB modeli %82,24 doğruluk oranına sahipken paralel ESA-UKSB modeli %82,89 doğruluk oranına sahip olduğu görülmüştür. AWID veri seti üzerinde hiyerarşik ESA-UKSB modeli %83,29 doğruluk oranına sahipken paralel ESA-UKSB modeli %98,30 doğruluk oranına sahip olduğu görülmüştür.

ESA ve UKSB sinir ağlarını bir araya getirmek, güçlü bir model oluşturmuştur. Her iki yaklaşımın da kendine özgü güçlü ve zayıf yönleri bulunmaktadır. Bu nedenle, en iyi seçimin, spesifik bir soruna bağlı olduğu sonucuna varılmaktadır.

Anahtar Kelimeler: Bulut Bilişim, Bulut Bilişim Güvenliği, Derin Öğrenme, Saldırı Tespit Sistemi

ABSTRACT

Analysis of Attacks on Cloud Computing with Deep Learning Method

Tuğba TEKKOL

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Software Engineering

October 2023, Pages: xi + 49

Cloud computing is a service model where computing resources such as servers, storage space, network infrastructure, data centers, and software services are provided over a shared network. This service model offers users flexibility, scalability, and cost savings. Despite the potential benefits of cloud computing, concerns about security have prevented individuals and businesses from fully embracing it. As a result, cloud computing security has become a new research topic.

Deep learning holds significant potential in the field of cloud computing security. As the complexity and volume of security threats increase, deep learning algorithms can play an effective role in detecting security vulnerabilities, preventing attacks, and ensuring data privacy within cloud systems. Deep learning-based analysis methods can examine large datasets to identify abnormal behaviors and enable prompt responses. These analyses often utilize neural network architectures.

In this thesis study, comprehensive research was conducted on the security issues in cloud computing. The challenges faced in the infrastructure-as-a-service model of cloud computing also affect other service models. Therefore, using deep learning techniques, various attack types and normal network traffic were monitored using extensive datasets named UNSW-NB15 and AWID, which represent network behaviors. Within the scope of the study, two models were created from neural network architectures commonly used in deep learning, namely Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM), which is a type of Recurrent Neural Network (RNN). In the first model, a hierarchical structure was employed where LSTM was used to learn the features of input data previously learned by CNN. In the second model, CNN and LSTM worked independently on the input data, and their outputs were merged in parallel. After training and testing these two models with the aforementioned datasets, the results were compared. It was observed that the hierarchical CNN-LSTM model had an accuracy rate of 82.24% on the UNSW-NB15 dataset, while the parallel CNN-LSTM model had an accuracy rate of 82.89%. It was observed that the hierarchical CNN-LSTM model had an accuracy rate of 83.29% on the AWID dataset, while the parallel CNN-LSTM model had an accuracy rate of 98.30%.

Combining CNN and LSTM neural networks appears to be a powerful model building method. Both approaches have their own strengths and weaknesses. Therefore, it follows that the best choice depends on the specific problem.

Keywords: Cloud Computing, Cloud Computing Security, Deep Learning, Intrusion Detection System

ŞEKİLLER LİSTESİ

	Sayfa
Şekil 2.1. Bulut Dağıtım Modelleri	7
Şekil 2.2. Bulut Hizmet Modelleri.....	7
Şekil 3.1. Derin Sinir Ağı Mimarisi [65].....	15
Şekil 3.2. Evrişimsel Sinir Ağı Yapısı [65].....	17
Şekil 3.3. Tekrarlayıcı Sinir Ağı Yapısı [65].....	17
Şekil 3.4. Tek Hücreli LSTM [72]	18
Şekil 4.1. UNSW-NB15 Veri Seti Sınıf Dağılımları	22
Şekil 4.2. AWID Veri Seti Sınıf Dağılımları.....	23
Şekil 4.3. Softmax Fonksiyonu [82].....	24
Şekil 4.4. 5 Kat Çapraz Doğrulama Örneği (a), 5 Katlı Katmanlı Çapraz Doğrulama Örneği (b)	25
Şekil 4.5. Paralel ESA-UKSB Tabanlı Modele Ait Katmanlar	26
Şekil 4.6. Hiyerarşik ESA-UKSB Tabanlı Modele Ait Katmanlar	27
Şekil 5.1. Hiyerarşik ESA-UKSB Modele Ait Karmaşıklık Matrisi (UNSW-NB15)	32
Şekil 5.2. Paralel ESA-UKSB Modele Ait Karmaşıklık Matrisi (UNSW-NB15).....	32
Şekil 5.3. Hiyerarşik ESA-UKSB Modeline Ait AİK-EAA Eğrisi (UNSW-NB15).....	33
Şekil 5.4. Paralel ESA-UKSB Modeline Ait AİK-EAA Eğrisi (UNSW-NB15).....	34
Şekil 5.5. Hiyerarşik ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (UNSW-NB15).....	34
Şekil 5.6. Paralel ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (UNSW-NB15).....	35
Şekil 5.7. Hiyerarşik ESA-UKSB Modele Ait Karmaşıklık Matrisi (AWID).....	36
Şekil 5.8. Paralel ESA-UKSB Modele Ait Karmaşıklık Matrisi (AWID).....	37
Şekil 5.9. Hiyerarşik ESA-UKSB Modeline Ait AİK-EAA Eğrisi (AWID).....	38
Şekil 5.10. Paralel ESA-UKSB Modeline Ait AİK-EAA Eğrisi (UNSW-NB15).....	38
Şekil 5.11. Hiyerarşik ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (AWID).....	39
Şekil 5.12. Paralel ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (AWID)	40

TABLÖLAR LİSTESİ

	Sayfa
Tablo 2.1. Bulutta Yaşanan Güvenlik Sorunları ve Alınan Önlemler.....	14
Tablo 5.1. Hiyerarşik ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (UNSW-NB15).....	31
Tablo 5.2. Hiyerarşik ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (UNSW-NB15).....	31
Tablo 5.3. Hiyerarşik ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (AWID).....	36
Tablo 5.4. Paralel ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (AWID)	36

SİMGELER VE KISALTMALAR

Kısaltmalar

ABD	: Amerikan Birleşik Devletleri
AİK	: Alıcı İşletim Karakteristiği
AWID	: Aegean Wi-Fi Intrusion Dataset
AWS	: Amazon Web Servisleri
BDH	: Basit Depolama Hizmetleri
BOATKA	: Balina Optimizasyon Algoritması Tabanlı Kategorik Arttırma
BT	: Bilgi Teknolojileri
ÇÖÇ-EÖM	: Çok Özellikli Çıkarma Ekstrem Öğrenme Makinesi
DHRS	: Dağıtılmış Hizmet Reddi Saldırıları
DN	: Doğru Negatif
DÖ	: Derin Öğrenme
DP	: Doğru Pozitif
DSA	: Derin Sinir Ağları
EAA	: AİK Eğrisi Altındaki Alan
EBİB	: Elastik Bilgi İşlem Bulutu
ESA	: Evrimsel Sinir Ağları
HOA	: Hizmet Olarak Altyapı
HOP	: Hizmet Olarak Platform
HOY	: Hizmet Olarak Yazılım
HRS	: Hizmet Reddi Saldırıları
KBA	: Kablosuz Bağlantı Alanı
NI	: Nesnelerin İnterneti
SM	: Sanal Makine
TSA	: Tekrarlayıcı Sinir Ağları
UİM	: Uluslararası İş Makineleri
UKSB	: Uzun Kısa Süreli Bellek
UNSW-NB15	: University of New South Wales-Network Based 15
UPA	: Uygulama Programlama Arayüzü
USTE	: Ulusal Standartlar ve Teknoloji Enstitüsü
ÜKÇOA	: Üstel Karıştırılmış Çoban Optimizasyon Algoritması
YBS	: Yapay Bağışıklık Sistemleri
YN	: Yanlış Negatif
YP	: Yanlış Pozitif

1. GİRİŞ

Günümüzde birçok alanda işletmeler, daha iyi müşteri hizmetleri sunmak için ve daha uygun maliyetli olması bakımından bilgi teknolojisini kullanmaktadırlar. Zamanla gelişmiş veya gelişmekte olan işletmelerin iş yoğunluğunun artması ile birlikte altyapılarını güçlendirmeleri gerekmektedir. Aksi takdirde bu işletmeler kullanıcılara gerekli platform ya da yüksek hız sunmak için yeterli olmayabilir. Bu bağlamda bilgi teknolojilerini güçlendirmek, üretkenliği arttırmak ve maliyetleri düşürmek için bulut bilişim kavramı ortaya çıkmıştır. Bulut bilişim, geleneksel bilgi teknolojilerine maliyet, hız ve performans bakımından üstün bir seçenek sunmaktadır.

ABD (Amerikan Birleşik Devletleri) Ulusal Standartlar ve Teknoloji Enstitüsü (USTE) tarafından yapılan tanıma göre bulut bilişim, yer ve zamandan bağımsız internet üzerinden ortak bir havuzla bilgisayar kaynaklarına (sunucular, depolama, ağ iletişimi, yazılım vs.) erişim sağlayan bir modeldir. Bu kaynaklar hızlı bir şekilde değiştirilebilir ve çok küçük bir yönetim çabası ile kullanılabilirler [1]. ABD merkezli çok uluslu bir teknoloji şirketi olan Microsoft tarafından yapılan tanıma göre ise bulut bilişim sunucular, depolama, veri tabanları, ağ sistemleri, yazılım, analitik sistemler gibi birçok bilgisayar servisinin internet üzerinden sağlanmasıdır. Bulut servis sağlayıcısı tarafından tıpkı evimizde kullandığımız su ve elektrik faturalandırılması gibi kullanıma dayalı olarak tarafımıza sunulmaktadır [2]. Dünyanın en büyük bilişim teknoloji şirketi olarak bilinen Uluslararası İş Makineleri (UİM) tarafından sunulan tanıma göre bulut, talep edilen bilgisayar kaynaklarının uygulamalardan başlayıp veri merkezlerine kadar birçok hususun internet üzerinden kullandıkça öde mantığıyla teslimatıdır. Bu kaynaklar ölçeklendirilebilir ve kullanıcı çevrimiçi bir kontrol panelinden ihtiyacına göre erişim sağlayabilir [3]. Son olarak Washington merkezli çok uluslu bir teknoloji şirketi olan Amazon tarafından yapılan tanıma göre bulut bilişim, kullanıcı talebi üzerine bilgisayar gücü, veri depolama, uygulamalar ve diğer BT (Bilgi Teknolojileri) kaynaklarının bir platform üzerinden kullandıkça öde mantığıyla sunulmasıdır [4].

Bilgi teknolojisi kullanan şirketlerin iki önemli konuyu göz ardı etmemeleri gerekmektedir. Bu konulardan birincisi maliyet planlaması olup şirketlerin faaliyetlerini sürdürebilmesi için dikkat edilmesi gereken önemli bir konudur. Bulut bilişim geleneksel yöntemlere göre hem zaman tasarrufu hem de uygun maliyet sağlamaktadır. Bulut servis sağlayıcısından alınan servis kullanımla paralel bir şekilde artış göstereceği için bulut bilişim esnek bir maliyet sunmaktadır. Şirketler tarafından bulut bilişim kullanıldığında donanım masrafı, personel masrafı ve bakım masrafı hızlıca azaltılabilir. Diğer bir önemli konu yönetim kavramıdır. Kullanılan geleneksel yöntemlerde mevcut sunucu sınıfına ek bir sunucu eklenmek istenildiğinde donanım maliyetine katlanmak zorunda kalılmaktaydı. Bulut bilişim var olan sınıfı sanallaştırarak yeni bir altyapı almayı kolaylaştırmaktadır. Bunun yanında sanal sunucular çevresel faktörlere karşı dayanıklı olmaktadır.

Bulut bilişimin kazandırdığı faydalar bilgi teknolojisi alanında devrim niteliğinde olmuştur. Ancak bulut bilişim geçmişine bakıldığında bulut sağlayıcının bulut yazılımındaki tasarım kusurları nedeniyle verilerin yanlışlıkla ele geçirildiği veya verilerin kasıtlı bir şekilde yayıldığı görülmüştür [5]. Bulut servis sağlayıcısı temin edilen hizmetlerde açıklık analiz testleri yapılamamakta bu yüzden güvenlik açıklıkları artmaktadır. Bulut ortamında veri gizliliği ve bütünlüğünü sağlamak, uygun kimlik doğrulama, yetkilendirme gibi göz önünde bulundurulması gereken birçok konu vardır [6].

Bulutun katmanlı yapısı düşünüldüğünde hem iç hem dış saldırılara karşı hassas olduğu görülmektedir [7]. Bulut kullanıcılarının ve bulut sağlayıcılarının verilerini siber saldırılara karşı korumak için güvenlik önlemleri alması gerekmektedir. Bulutta yaşanan güvenlik sorunlarının önüne geçmek ve buluta olan güveni kazandırmak için birçok çalışma yapılmıştır. Victor R. Kemande ve Hein. S. Venter botnet saldırılarının her geçen gün geliştirildiğini ve bulutta algılamanın zorlaştığını ifade etmişlerdir. Bu sorunun çözümü için Yapay Bağışıklık Sistemleri (YBS) kullanan bir tespit mekanizması sunmuşlardır. Bu mekanizma kötü amaçlı bir kod kalıbı algıladığında filtreleyip bunun bir saldırı olduğunu bildirmektedir [8]. Başka bir çalışmada Opeyemi Osaniye vd. Dağıtılmış Hizmet Reddi Saldırıları (DHRS) konusuna odaklanmışlardır. DHRS saldırılarının bulutun bant genişliğini, hizmetlerini ve kaynaklarını hedef alarak bulutu kullanılmaz hale getirdiğini ifade etmişlerdir. Yapılan çalışmada saldırı tespiti için yaygın olarak kullanılan NSL-KDD veri seti kullanılmıştır. 41 özellikli tam veri setini, 14 özellikli filtre yöntemlerinin üçte birlik bölümünü ve 13 özellikli çoklu filtre özelliği seçim yöntemini kullanan J48 sınıflandırıcısının performans ölçümünün sonuçlarını sunmuşlardır [9].

Bulut bilişim mimarisinin temelinde sanallaştırma kavramı yatmaktadır. Sanallaştırma bulutun temel yapı taşı olup beraberinde bazı güvenlik sorunlarını da getirmektedir. Fengzhe Zhank vd. sanal makinenin (SM) canlı geçişi sırasında gizlilik ve bütünlüğün korunması gerektiğini ifade etmişlerdir. Yaptıkları çalışmada SM'lerin canlı geçişi için PALM adında Xen ve GNU Linux tabanlı bir koruma kalkını prototipi oluşturmuşlardır. Oluşturulan prototipi tipik sunucu uygulamaları ile karşılaştırıldığında canlı geçişteki performans düşüşünün hafif olduğunu gözlemlemişlerdir [10]. P. Neelakantan SM'yi kötü amaçlı isteklerden korumak ve bulutta bağlı sanal SM'lerin güvenliğini sağlamak için Balina Optimizasyon Algoritması Tabanlı Kategorik Arttırma (BOATKA) adında bir mekanizma önermiştir. Önerilen mekanizmanın güvenliğini kontrol etmek için sisteme kötü amaçlı istek göndererek zaman, gizlilik, hata tespit oranı, veri paylaşım ölçüsü ve kaynak kullanımı açısından diğer modellerle karşılaştırmıştır. Çalışma sonucunda BOATKA, verileri yürütmek için daha az zaman ve yüksek saldırı tespit oranı elde etmiştir [11].

2019 yılında Mohamed Jelidi vd. tarafından yayımlanan başka bir çalışmada bulutun önemli katmanlarını korumak için hibrit bir saldırı tespit sistemi sunulmuştur. Önerilen saldırı tespit modeli

iki bölgeye ayrılmıştır. Birinci bölge, imza tabanlı detektörlerle ikinci bölge ise anomali tabanlı detektörlerle donatılmıştır. İlk bölgede önceden bilinen saldırıların tespitini yapmayı hedeflemişlerdir, ikinci bölgede ise önceden bilinmeyen kötü amaçlı etkinlikleri keşfetmeye çalışmışlardır. Modele uygulanan ataklar sonucunda bu tür saldırı tespit sisteminin kullanılmasının fayda sağladığı görülmüştür [12]. Preeti Mishra vd. ağ ve sanallaştırma katmanındaki güvenlik sorunlarına dikkat çekmiştir. Bahsi geçen katmanlarda yaşanan izinsiz girişlerle başa çıkmak için NvCloudIDS adında bir güvenlik mimarisi önermişlerdir. NvCloudIDS, bulut ağ sunucusuna gelen ve giden ağ trafiğinin davranışsal analizini gerçekleştirmekte ve ağ düzeyinde gerçekleşen izinsiz girişlere karşı savunma sağlamaktadır. Aynı zamanda sanal makine bellek iç gözlemi ve sanal makine trafik analizini gerçekleştirmektedir. Oluşturulan mimari UNSW-NB15 adında bir saldırı veri seti ile doğrulanmıştır ve elde edilen sonuçların umut verici olduğu görülmüştür [13]. El-Kassabi vd. bulut iş akışı düzenlemelerinde oluşan anormallikleri tespit veya tahmin etmek için derin öğrenme, sınıflandırma ve kümelemeyi birleştiren bir mimari ile bulut kaynaklarının, iş akış görevlerinin ve verilerin izlenmesini vurgulamışlardır. Çalışma değerlendirilmeleri sonucunda oluşturulan mimari denetlenmeyen statik ve dinamik özellikleri yakalayıp veri boyutunu azaltmıştır. Böylece potansiyel saldırıların daha iyi tahmin edilmesi sağlanmıştır [14].

Son zamanlarda araştırmacılar tarafından ağ izinsiz girişlerini bulmak için çeşitli algılama yaklaşımları önerilmiştir. Anıl Kumar vd. bilgisayar ağlarındaki gelişmelerin (E-ticaret, Bulut Altyapıları, Nesnelerin internetinde gelişmeler) hayal edilemeyecek kadar erişime izin verdiğini ileri sürmüşlerdir. Bu sorunla baş edebilmek için bulanık mantık ve derin öğrenme ikilisini kullanan bir saldırı tespit şemasının metodolojisini açıklamışlardır. Önerdikleri saldırı tespit sistemi performansı literatürde belirlenen son teknoloji yaklaşımlarla karşılaştırılmıştır. Oluşturdukları modelin izinsiz giriş tespitinin doğruluk oranını arttırdığını ve daha düşük hata oranı sağladığını açıklamışlardır [15]. B. K. Pandey vd. Üstel Ağırlıklı Hareketli Ortalama ve Karışık Çoban Optimizasyon Algoritması birleştirilerek ÜKÇOA (Üstel Karıştırılmış Çoban Optimizasyon Algoritması) kullanılarak izinsiz giriş tespiti için bir derin öğrenme yaklaşımı önermişlerdir. Önerilen model MQTT-IOT-IDS2020 veri seti ve Apache Web Sunucusu veri seti kullanılarak incelenmiştir. Apache Web Sunucusu veri setini kullanan deneysel sonuçlara göre ÜKÇOA 0.883 doğruluk oranı sunmuştur [16].

Son dönemlerde yapay zekâ ile birlikte gelen makine öğrenmesi, derin öğrenme gibi çalışma alanları birçok alanda kullanıldığı gibi saldırı tespit çalışmalarında da kullanılmaya başlanmıştır. Literatürde derin öğrenme teknikleri kullanılarak anomali saldırı tespiti yapılan birçok çalışma bulunmaktadır. Devrim Akgün vd. tarafından yürütülen bir çalışmada bulut güvenliği için oluşturulan saldırı tespit sisteminde Evrişimli Sinir Ağları (ESA) ve Tekrarlayıcı Sinir Ağları (TSA) kullanılarak yeni bir derin öğrenme modeli geliştirilmiştir. Geliştirilen bu model NSL-KDD adında bir veri seti kullanılarak eğitilmiştir. Eğitimden sonra test edilen modelin %99,86 doğruluğa

sahip olduğu gözlemlenmiştir [17]. Haifeng Lin vd. nesnelerin interneti (Nİ) ve geleneksel internet karşılaştırıldığında Nİ'nin büyük varlıklar, karmaşık ve çeşitli yapılar ve bilgi işlem kaynaklarının eksikliği gibi birçok sorununun bulunduğunu ifade etmişlerdir. Bu nedenle geleneksel ağ saldırı tespit sistemlerinin, Nİ uygulamalarının güvenlik ihtiyaçlarını karşılayamadığını öne sürmüşlerdir. Var olan problem ışığında yapılan bu çalışma bulut bilgi işlem, gelişmiş bir aşırı öğrenme makinesi ve diğer yöntemleri kullanarak bulut bilgi işlem ortamlarında Nİ izinsiz girişi algılamayı ve bulut düğüm izlemeyi kapsamlı bir şekilde araştırmaktadır. Çalışma kapsamında Çok Özellikli Çıkarma Ekstremler Öğrenme Makinesi (ÇÖÇ-EÖM) algoritması kullanılmıştır. Deneyler sonucunda önerilen algoritmanın çoğu ağ veri paketini algılayıp tanımlayabildiğini ve Nİ'nin heterojen verileri için verimli bir izinsiz giriş tespiti gerçekleştirebildiği görülmüştür [18]. Peilun Wu ve Hui Guo tarafından ağa yapılan izinsiz girişleri zamanında yakalayabilmenin kritik olduğu belirtilmiştir. Yapılan çalışmada izinsiz giriş tespiti için ESA ve TSA sinir ağlarını kullanarak LuNet adında hiyerarşik bir sinir ağı önerilmiştir. LuNet'in doğruluğunu test etmek için NSL-KDD ve UNSW-NB15 adlı veri setleri kullanılmıştır. Çalışma sonucunda LuNet'in hem yüksek düzeyde algılama kapasitesi sunduğunu hem de çok düşük yanlış algılama oranına sahip olduğu öne sürülmüştür [19].

Bu tez çalışmasında bulutta yaşanan güvenlik sorunları ele alınmakta ve buluta karşı yapılan saldırılar derin öğrenme teknikleriyle tespit edilmeye çalışılmaktadır. Çalışma kapsamında çeşitli saldırı türlerini ve normal ağ trafiğini temsil eden iki geniş veri kümesi olan UNSW-NB15 ve AWID kullanılmaktadır. Bu veri setleri derin öğrenme alanında yaygın olarak kullanılan ESA ve TSA'nın bir türü olan UKSB (Uzun Kısa Süreli Bellek) sinir ağlarından iki model oluşturularak eğitilip test edilmiştir. İlk modelde UKSB'nin, ESA tarafından öğrenilmiş olan girdi verilerinden özellikleri öğrenmesini sağlamaktadır. İkinci modelde ise ESA ve UKSB'nin girdi verileri üzerinde bağımsız olarak çalıştığı ve çıktıların birleştirildiği paralel bir model sunulmaktadır. Bu iki model yukarıda bahsettiğimiz veri setleri ile eğitilip test edildikten sonra sonuçlar karşılaştırılmaktadır.

2. BULUT BİLİŞİM

Son yıllarda hızla gelişen dijital dünyada, bilgi işlem teknolojileri sürekli olarak ilerlemekte hayatımızı kolaylaştırmak için yeni çözümler sunmaktadır. Bu çözümlerden biri de günümüzde çoğu işletme ya da bireyler tarafından kullanılan bulut bilişim teknolojisidir. Bulut bilişim, bilgisayar işlemi ve depolama olmak üzere iki önemli ihtiyaca cevap vermektedir. Bu önemli ihtiyaçlar, kullanıcılara herhangi bir zaman ve mekândan bağımsız olarak sunulmaktadır.

Bulut bilişimin tarihine baktığımızda, 1950'li yıllarda büyük ölçekli ve pahalı bilgisayarlar bulunmaktaydı. Ancak bu bilgisayarlara erişmek, taşınması zor ve yüksek maliyetli oluşu nedeniyle herkes için mümkün değildi. Bu sorunu çözmek için John McCarthy tarafından öne sürülen, zaman paylaşımlı olarak adlandırılan bir kavram ortaya çıkmıştır [20]. Bu kavram sayesinde, kullanıcılar bu büyük bilgisayarlardan faydalanabilmek için zaman paylaşımı yöntemini kullanarak işlem gücünü belli bir ücret karşılığında kullanmaya başladı. Bu sayede, küçük şirketler bile belirli bir ücret karşılığında bilgisayar işlem gücüne erişebilme imkânı buldular.

1960'ların ortasına gelindiğinde, Amerikalı bilim insanı Licklider tarafından öne sürülen internetin temelini oluşturan ARPANET kavramıyla birlikte bilgisayarların birbirlerine bağlanması fikri ortaya çıktı [21]. 1970'lerden itibaren bulut bilişimin gereksinim duyduğu birçok teknoloji ortaya çıkmaya başladı. Bu dönemde UİM'in sanal makine kavramını işletim sistemi olarak geliştirmesi bu teknolojilerin öncüsüydü. Daha sonra telekomünikasyon şirketleri de kendi sanal özel ağlarını oluşturarak bu gelişmelere katkıda bulundular. 1990'ların ortalarında arama motorları (Yahoo, Google) ve e-posta hizmetleri (Hotmail, Gmail) gibi teknoloji araçları ortaya çıktı. 1997 yılında Chellappa, bulut bilişimin ilk tanımını yaparak bilgisayar işlemlerinin sadece teknik sınırlardan değil, ekonomik gerekçeyle belirlenecek bir hesaplama paradigması olduğunu belirtti [22].

1999 yılında Salesforce.com, bulut bilişimin gelişimi yolunda kurulan ilk şirket oldu. 2002'de Amazon Web Servisleri (AWS), bulut bilişim sektöründe öncü bir şirket olarak kuruldu. 2006 yılında ise en önemli ihtiyaçlardan biri olan bilgisayar işlem gücü ve depolama ihtiyacına cevap vermek amacıyla Amazon Elastik Bilgi İşlem Bulutu (EBİB) ve Basit Depolama Hizmetleri (BDH) kullanıcılara sunuldu [23].

Bu gelişmelerin sonucunda bulut bilişim, iş dünyasında ve teknoloji alanında büyük bir etki yaratmıştır. Ölçeklenebilirlik, esneklik, maliyet tasarrufu ve kolay erişim gibi avantajlarıyla bulut bilişim, günümüzde birçok şirketin ve kullanıcının tercih ettiği bir hizmet modeli haline gelmiştir. Gelecekte, bulut bilişimin daha da gelişerek yeni yeniliklere yol açması beklenmektedir.

2.1. Bulut Dağıtım Modelleri

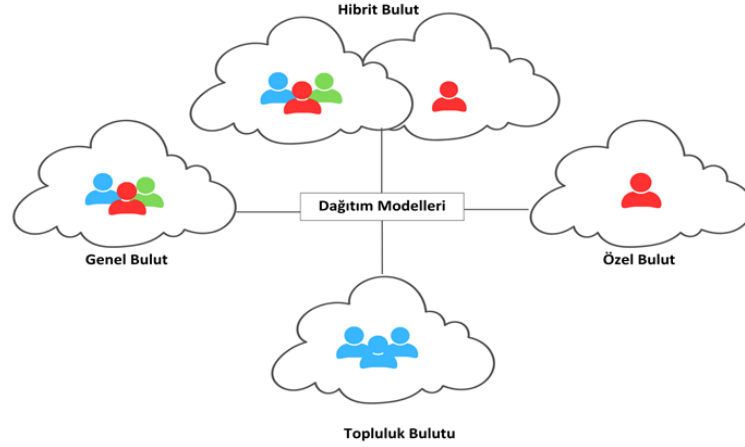
Bulut bilişim, günümüzde birçok işletmenin veya bireylerin bilgisayar işlemi ve veri depolama ihtiyaçlarını karşılamak için tercih ettiği bir teknolojidir. Bulut bilişim, internet üzerinden sunulan kaynaklara erişim sağlayarak, kullanıldığı kadar ödeme sağlanabilecek modeliyle ölçeklenebilirlik, esneklik ve verimlilik sağlamaktadır. Bulut bilişim hizmetleri sunan sağlayıcılar, bulut kullanıcılarının kaynakları en etkin ve verimli şekilde kullanabilmeleri için çeşitli dağıtım modellerini kullanıcılara sunmaktadır [24]. Bu dağıtım modelleri Şekil 2.1’de görülmektedir.

Genel Bulut: Genel bulut, birden fazla kullanıcının ve kuruluşun aynı altyapıyı paylaştığı dağıtım modelidir. Bu tür dağıtım modeli hizmetine herkes tarafından erişilebilmektedir [25]. Genel bulut hizmet sağlayıcıları, içinde sunucular, depolama alanı, ağ altyapısı ve diğer bilişim kaynakları olan büyük ölçekli merkezler oluşturmaktadır. Kullanıcılar, bu hizmet sağlayıcıların sunucularına uzaktan erişim sağlayarak kaynaklara ulaşabilir ve ihtiyaçlarına göre bu kaynakları kullanabilmektedir. Kaynakların tam kontrolünü sağlamak veya altyapıyı özelleştirmek isteyen kullanıcılar için bu dağıtım modeli uygun olmayabilir [24, 25].

Özel Bulut: Özel bulut, sadece bir işletmenin kullanımı için tasarlanmış özel bir altyapıdır. Kullanıcı, kendi veri merkezi içerisinde veya üçüncü taraf bir sağlayıcının veri merkezinde özel bulutunu barındırabilir [26]. Özel bulut, kuruluşlara daha fazla güvenlik, kontrol ve özelleştirme imkânı sağlar. Bununla birlikte, özel bulutun daha yüksek maliyetleri ve yönetim gereksinimleri bulunmaktadır.

Hibrit Bulut: Hibrit bulut, genel bulut ve özel bulutun özelliklerini birleştirerek oluşturulan bir dağıtım modelidir. İşletmeler, önemli verileri ve iş uygulamalarını özel bulutta saklayabilirken, kritik bir öneme sahip olmayan diğer verileri genel bulutta depolayabilmektedir. Hibrit bulut, güvenlik ve kontrol gerektiren iş yüklerini özel buluta yerleştirirken, ölçeklenebilirlik ve esneklik avantajlarından da yararlanmayı sağlayan bir yapıya sahiptir [25].

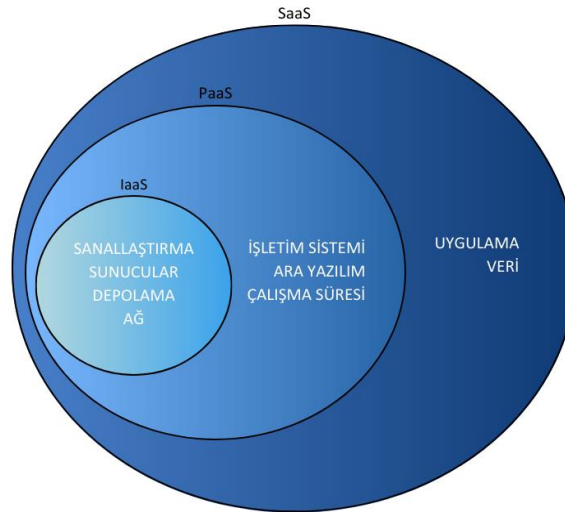
Topluluk Bulutu: Topluluk bulutu, belli bir meslek veya iş birliği içindeki bir grup kurulaşa özgü olarak oluşturulan bir bulut dağıtım modelidir. Toplanmış bulut, kaynakları paylaşarak maliyetleri düşürmeyi ve iş birliği ile veri paylaşımını kolaylaştırmayı amaçlamaktadır. Bu model, grup üyeleri arasında daha güçlü bir iş birliği ve veri entegrasyonunu teşvik ederek operasyonel verimliliği artırmasını sağlar. Topluluk bulutu, güvenlik, uyumluluk ve özelleştirme konularında grup üyelerine daha fazla kontrol imkânı sağlamaktadır. Bu şekilde, kuruluşlar ortak gereksinimleri olan bir topluluk içinde iş birliği yapabilmekte ve daha etkili bir şekilde kaynakları paylaşabilmektedir [27].



Şekil 2.1. Bulut Dağıtım Modelleri

2.2. Bulut Hizmet Modelleri

Bulut hizmet modelleri, kullanıcıların ihtiyaçlarına ve isteklerine göre farklı seviyelerde hizmet sunmaktadır. Bu hizmet modelleri yönetim, ölçeklenebilirlik, geliştirme ve maliyet gibi konularda kullanıcının ihtiyacına göre yanıt vermek için tasarlanmıştır [28]. Örneğin, bazı kullanıcılar işletim sistemi, uygulamalar ve verileri yönetmek isterken, diğerleri sadece verilerini yönetmeyi tercih edebilir. Bu farklı ihtiyaçlara cevap vermek için farklı bulut hizmet modelleri oluşturulmuştur. Şekil 2.2’de Bulut hizmet modellerinin hangi isteğe karşılık verebileceği gösterilmektedir.



Şekil 2.2. Bulut Hizmet Modelleri

2.2.1. Hizmet Olarak Altyapı

Hizmet Olarak Altyapı (HOA), bulut bilişim hizmetlerinin en alt seviyesinde bulunmakta ve kullanıcılara sanal altyapı kaynakları sunmaktadır. Bu modelde kullanıcılar geleneksel fiziksel

altyapı yerine sanal olarak sunulan kaynaklara erişebilmektedir. Sunucular, depolama, ağ bileşenleri ve diğer altyapı kaynakları, kullanıcılara ihtiyaçlarına göre sağlanmaktadır. Kullanıcılar, kendi işletim sistemlerini, uygulamalarını ve verilerini bu sanal altyapı üzerinde çalıştırabilmektedir [28, 29].

Bu hizmet modeli, maliyet tasarrufu, hızlı ölçeklendirme ve daha verimli iş süreçleri gibi bir dizi avantaj sunmaktadır. İşletmelerin taleplerine göre altyapıyı genişletebilmesine veya küçültebilmesine olanak tanımakta ve uygun bir altyapı sağlama esnekliği sunmaktadır. Kullanıcılar, altyapı kaynaklarını paylaşılan bir ortamda kiralayıp ve sadece kullandıkları kaynaklar için ödeme yapmaktadır. Bu sayede, fiziksel altyapı yatırımına büyük bütçeler ayırma zorunluluğu ortadan kalkmaktadır.

HOA sağlayıcıları, fiziksel altyapının bakımı, güncellemeleri ve güvenliği gibi görevleri üstlenmektedir. Bu, kullanıcıların altyapı yönetimiyle ilgili sorumluluklarını azaltmakta ve işletmelerin kaynaklarını daha stratejik hedeflere odaklamalarını sağlamaktadır.

2.2.2. Hizmet Olarak Platform

Hizmet Olarak Platform (HOP), kullanıcılara uygulama geliştirme ve dağıtım için bir platform sağlayan bulut bilişim hizmet modelidir [30]. HOP, işletim sistemleri, veri tabanları, geliştirme araçları, web sunucusu ve diğer çeşitli yazılım bileşenlerini içeren bir platformu hizmet olarak sunmaktadır. Bu sayede kullanıcılar, uygulama geliştirme sürecine odaklanabilir ve altyapı yönetimi gibi ayrıntılarla uğraşmak zorunda kalmazlar. HOA'dan farklı olarak HOP, işletmelere uygulama geliştirmek için gereken tüm araçları ve altyapıyı sağlamaktadır. Bu sayede geliştiriciler, hızlı bir şekilde uygulama geliştirme sürecine başlayabilir ve mevcut bileşenleri kullanarak daha iyi sonuçlar elde edebilir [29].

HOP, kullanıcıların uygulama geliştirmeye ve yenilikçi fikirleri hayata geçirmeye odaklanmasını sağlayan güçlü bir hizmet modelidir. İşletmeler, HOP'un sunduğu avantajları kullanarak rekabet avantajı elde edebilir ve hızla değişen teknolojilere uyum sağlayabilir.

2.2.3. Hizmet Olarak Yazılım

Hizmet Olarak Yazılım (HOY), kullanıcılara internet üzerinden yazılım uygulamalarına erişim sağlayan bir bulut bilişim hizmet modelidir. Bu modelde, yazılım bir hizmet sağlayıcı tarafından barındırılmakta ve yönetilmekte, kullanıcılar ise web tarayıcısı aracılığıyla kurulum veya altyapı yönetimi gerektirmeden erişebilmektedir [31]. HOA ve HOP'tan farklı olarak HOY, yazılım uygulamalarını internet üzerinden bir hizmet olarak sunmaktadır. Kullanıcılar, yazılımı yerel cihazlarına kurulum veya güncelleme yapmadan web tarayıcısı aracılığıyla erişip kullanabilmektedir.

HOY, işletmelere daha düşük maliyetler, hızlı uygulama dağıtımı, kullanım kolaylığı, ölçeklenebilirlik, otomatik güncellemeler ve iş birliği için kolay erişim gibi bir dizi avantaj sunar. Bu nedenle, birçok işletme müşteri ilişkileri yönetimi, kurumsal kaynak planlaması, insan kaynakları yönetimi, proje yönetimi ve iş birliği araçları gibi çeşitli alanlarda hizmet olarak yazılım desteği almaktadır [32].

2.3. Bulutta Yaşanan Güvenlik Sorunları

Bulut bilişim, işletmelerin veri depolama ve işleme gibi işlemlerini gerçekleştirmesinde devrim niteliğinde bir yenilik getirmiştir. Esnek oluşu, ölçeklenebilir oluşu, maliyet tasarrufu ve yüksek verimlilik gibi birçok özelliğinden dolayı dünya çapında hızlı bir yayılım göstermeye başlamıştır. Ancak diğer tüm teknolojik gelişmeler gibi, bulut bilişim de kendi güvenlik kaygılarıyla birlikte gelmiştir. Bu durum, işletmelerin zihninde soru işaretleri yaratmış ve bulut pazarının büyümesini engellemiştir.

Bulut bilişimin güvenlik sorunları, yeni bir çalışma alanını ortaya çıkarmıştır. Bu sorunlar üzerinde birçok araştırmacı çalışmalar yapmış ve hâlâ yapmaktadır. Bulutta yaşanan başlıca güvenlik sorunları arasında veri ihlalleri, güvensiz ara yüzler/UPA'lar (Uygulama Programlama Ara Yüzleri), yetersiz kimlik ve erişim yöntemi, üçüncü taraf ilişkileri, Hizmet Reddi Saldırıları (HRS) ve paylaşılan teknoloji açıkları gelmektedir [33]. Güvenlik sorunlarına önlem almak adına yaşanan sorunlar gruplandırılarak üzerinde durulmuştur.

2.3.1. Hizmet Olarak Altyapı Modelinde Yaşanan Güvenlik Sorunları

HOA, işletmelere sanal bir altyapı sunarak, donanım kaynaklarını sanal olarak sağlamaktadır. HOA sağlayıcıları, müşterilere genellikle bir kullanıcı ara yüzü veya UPA aracılığıyla sanal sunucuları yönetme imkânı sunmaktadır. Müşteriler, bu sanal sunucuları taleplerine ve ihtiyaçlarına göre yönetebilmektedir. Sanal sunucular, işletim sistemleri, uygulama yazılımları ve veri tabanları gibi çeşitli iş yüklerini barındırmaktadır. Saldırganlar, sürekli olarak yeni yöntemler ve teknikler geliştirerek, HOA altyapısını hedef alan saldırıları gerçekleştirme potansiyeline sahiptir. Bu nedenle hem HOA sağlayıcılarının hem de müşterilerin, güvenlik önlemlerini sürekli güncellemek, zayıf noktaları tespit etmek ve uygun güvenlik önlemlerini almak için dikkatli olmaları gerekmektedir. Yapılan literatür taraması sonucunda, HOA modelinde saldırıların potansiyel olarak istismar edebileceği alanlara aşağıda değinilmektedir.

Zayıf Kimlik Doğrulama ve Erişim Kontrolleri: Kimlik doğrulama, kullanıcıların veya sistemlerin kimliklerini kanıtlamak için kullanılan bir süreçtir. HOA ortamında, zayıf kimlik doğrulama, kullanıcıların güçlü parolalar kullanmaması, çok faktörlü kimlik doğrulama yöntemlerini kullanmaması veya kimlik doğrulama sürecinin zayıf olması gibi durumları

içermektedir [34]. Saldırganlar, kullanıcı adı ve şifre gibi kimlik bilgilerini ele geçirerek yetkisiz erişim sağlayabilmektedir. Erişim kontrolleri, kullanıcıların ve sistemlerin kaynaklara erişimini kontrol etmek için kullanılan politika ve mekanizmalardır. HOA ortamında yetersiz erişim kontrolleri, doğru yetkilendirmenin yapılmaması, kullanıcı rollerinin düzgün tanımlanmaması veya hizmetlere erişimi sınırlamak için gerekli kontrollerin eksik olması gibi durumları içermektedir. Bu sorunlar, saldırganların yetkisiz erişim elde etmesine ve HOA hizmetlerine izinsiz olarak erişmesine olanak sağlayabilmektedir.

Paylaşımlı Altyapı: HOA modelinde, müşteriler paylaşımlı yapısı nedeniyle altyapı, sunucular, depolama birimleri, ağ bileşenleri ve diğer kaynakları paylaşmaktadır. Her müşteri, kendi sanal ortamını oluşturmak için bu paylaşımlı altyapıyı kullanmaktadır. Paylaşımlı altyapı, işletmelere maliyet tasarrufu, esneklik ve ölçeklenebilirlik sağlarken, bazı güvenlik risklerini beraberinde getirmektedir. Bir müşterinin güvenlik açığı veya saldırıya uğraması, diğer müşterileri ve kaynakları da etkileyebilmektedir [35]. Örneğin, bir müşterinin sanal makinesindeki bir güvenlik açığı saldırganlara yetkisiz erişim sağlayabilir. Bu durumda, saldırganlar diğer müşterilerin verilerine veya kaynaklarına zarar verebilir veya saldırı gerçekleştirebilir. Ayrıca, bir müşterinin yoğun trafik veya kaynak talebi, diğer müşterilerin hizmet kalitesini etkileyebilir.

Yetersiz Yapılandırma: İşletmeler, HOA sağlayıcısı tarafından sunulan altyapıyı doğru bir şekilde yapılandırmalı ve güncellemeleri düzenli olarak uygulamalıdır. Yetersiz yapılandırma, yetkisiz erişime veya veri kaybına neden olabilmektedir [36]. Sağlayıcı tarafından sunulan kontrol paneli veya yönetim araçları doğru bir şekilde kullanılmalıdır. Ayarlarında hatalı yapılandırmalar veya eksiklikler olması, güvenlik açıklarına neden olabilmektedir. İşletmelerin, güçlü parola politikalarını uygulaması, çok faktörlü kimlik doğrulama yöntemlerini kullanması ve kullanıcı hesaplarının güvenliğini sağlamak için gereken diğer önlemleri alması oldukça önemlidir. Aksi takdirde, saldırganlar zayıf kimlik doğrulama bilgilerini kırabilir veya ele geçirebilir. Bir diğer açık yetkilendirme ve erişim haklarının yanlış yapılandırılması olup, yetkisiz kullanıcıların hassas verilere erişim sağlamasına veya altyapıyı manipüle etmesine olanak tanımaktadır. İşletmeler, kullanıcı rolleri ve izinleri doğru bir şekilde ayarlamalı, gereksiz ayrıcalıkları kaldırmalı ve ilke tabanlı erişim kontrolü politikalarını uygulamalıdır. Son olarak HOA sağlayıcısı tarafından sağlanan altyapı ve yazılımların güncellemeleri düzenli olarak takip edilmelidir. Eksik güncellemeler, bilinen güvenlik açıklarını kapatmayı engeller ve saldırganların sisteme sızma veya saldırı gerçekleştirme olasılığını artırır. İşletmelerin, güncelleme politikalarını belirlemesi ve güncellemeleri düzenli olarak uygulaması gerekmektedir [29, 36].

İzleme ve Tehdit Tespiti: İzleme ve tehdit tespiti eksikliği, güvenlik açıklarının kaçırılmasına, yanıt süresinin yavaşlamasına, veri kaybına, uyumluluk sorunlarına ve saldırı analizi eksikliğine neden olabilmektedir [37]. İzleme sistemleri, normal işleyişe göre anormal etkinlikleri tespit etmektedir. Bu, saldırganların veya kötü amaçlı yazılımların sisteme sızma girişimlerini veya

zararlı aktivitelerini belirlemede yardımcı olmaktadır. Anormal aktivitelerin tespiti, potansiyel saldırıları erken aşamada fark etmek ve buna göre önlem almak için kritiktir.

2.3.2. Hizmet Olarak Platform Modelinde Yaşanan Güvenlik Sorunları

HOP güvenliği, kullanıcıların ve hizmet sağlayıcıların güvenliği sağlamak için dikkate almaları gereken birçok konu barındırmaktadır. Bunlar arasında zayıf kimlik doğrulama ve erişim kontrolleri, veri güvenliği, uygulama katmanı güvenliği, paylaşımlı ortamın riskleri, veri yedekleme/kurtarma ve hizmet sağlayıcı güvenliği yer almaktadır [38]. HOP kullanıcıları, doğru kimlik doğrulama mekanizmalarını kullanmalı, verilerini şifrelemeli, uygulamalarını güvenlik açıklarına karşı tarayarak güvence altına almalı ve hizmet sağlayıcılarıyla iş birliği yaparak güvenli bir ortam sağlamalıdır. Aynı zamanda, hizmet sağlayıcılarının güvenlik önlemlerini yeterli düzeyde uygulaması ve düzenli olarak güncellemeleri de önemlidir. HOP güvenliği, kullanıcıların verilerini ve uygulamalarını korumak, yetkisiz erişimleri önlemek ve güvenli bir bulut bilişim deneyimi sunmak için sürekli olarak gözden geçirilmeli ve geliştirilmelidir. Taramalar sonucunda, aşağıda HOA modelinde yaşanabilecek güvenlik sorunlarının genel başlıkları yer almaktadır.

Temel Altyapı Güvenliği: HOP modelinde, kullanıcılar uygulama geliştirme ve dağıtım için bir platformu kullanırken, altyapının güvenliği sağlayıcı tarafından yönetilir. Bu, kullanıcıların verilerinin ve uygulamalarının güvende olmasını sağlamak amacıyla çeşitli önlemler gerektirir [39].

Paylaşımlı Ortam Sorunları: HOP, birden çok kullanıcının aynı altyapıyı paylaştığı bir ortam sağlar. Bu durumda, bir kullanıcının güvenlik açığı veya saldırıya uğraması diğer kullanıcıları ve hizmet sağlayıcıyı etkileyebilir. İzolasyonun yetersiz olması veya güvenlik önlemlerinin eksikliği, saldırganların diğer kullanıcılara sızmasına ve saldırılarını genişletmelerine olanak tanıyabilir. Kötü niyetli bir kullanıcının veya saldırganın bir hesaba karşı saldırı gerçekleştirmesi durumunda, diğer kullanıcılar ve hizmet sağlayıcı risk altında olabilir. İzolasyonun yetersiz olması, saldırganın diğer kullanıcıların verilerine veya uygulamalarına erişebilmesine olanak sağlayabilmektedir [38, 40].

Üçüncü Taraf İlişkileri: HOP sağlayıcısı tarafından kullanılan hizmet sağlayıcıları veya dış kaynaklar aracılığıyla ortaya çıkabilir. Örneğin, veri depolama, veri tabanı hizmetleri, kimlik doğrulama veya analitik araçları gibi hizmetler üçüncü taraf sağlayıcılar tarafından sağlanabilir. Bu durumda, kullanıcılar verilerini bu üçüncü taraf hizmet sağlayıcılarına aktarmak durumunda kalabilir. Bu durum, güvenlik ve gizlilik konularında bazı riskleri beraberinde getirebilir [40, 41]. Kullanıcılar, üçüncü taraf hizmet sağlayıcılarına güvenmek zorundadır ve bu sağlayıcıların güvenlik politikalarını, veri koruma önlemlerini ve uyumluluk durumlarını dikkatlice değerlendirmeleri önemlidir. Ayrıca, kullanıcılar, verilerinin üçüncü taraflarla paylaşılıp paylaşılmadığı, izinsiz erişim riskleri ve veri gizliliği konularında endişeler taşıyabilirler.

2.3.3. Hizmet Olarak Yazılım Modelinde Yaşanan Güvenlik Sorunları

HOY modelinde, kullanıcılar uygulamaları ve verileri bulut tabanlı bir hizmet sağlayıcının sunucusunda barındırırlar. Bu durumda, kullanıcılar ve verileri dışarıdan erişilebilir hale gelir, bu da çeşitli güvenlik sorunlarını beraberinde getirir. Bu tür bir ortamda veri gizliliği riski, veri güvenliği zayıflığı, hizmet kesintileri, zayıf kimlik doğrulama veya erişim kontrolleri ve hizmet sağlayıcının güvenliği gibi kullanıcı bilgilerine zarar verecek birçok sorun bulunmaktadır [40]. Bu sorunlar hakkında aşağıda daha detaylı bilgi verilmiştir.

Veri Güvenliği: HOY modelinde kullanıcılar, veri güvenliği konusunda bazı sorunlarla karşılaşabilmektedir. Kullanıcıların verileri hizmet sağlayıcının altyapısında depolanır ve işlenir, bu da kullanıcıların verilerine dışarıdan erişim sağlanabileceği anlamına gelir. Bu durumda, kullanıcılar veri güvenliği konusunda bazı endişeler yaşayabilirler. Özellikle, veri gizliliği ve güvenliği, kullanıcıların verilerinin yetkisiz kişilerin eline geçmesi veya kötü niyetli saldırılara maruz kalması gibi sorunlarla karşılaşılabilir [42].

Kimlik Doğrulama ve Erişim Kontrolleri: HOY hizmetlerinde, kullanıcıların kimlik doğrulama ve erişim kontrolleri konusunda yeterli önlemler almaları büyük önem taşımaktadır. Zayıf veya kolay tahmin edilebilir parolaların kullanılması, hatalı yetkilendirme ayarlarının yapılması veya kötü niyetli kullanıcıların hesaplara yetkisiz erişim girişimleri gibi durumlar, yetkisiz erişimlere ve hesapların ele geçirilmesine yol açabilir. Bu da kullanıcının verilerinin ve uygulamalarının güvenliğini tehlikeye atmaktadır. Ayrıca, hatalı yetkilendirme ayarları veya yanlış yapılandırılmış erişim kontrolleri, kullanıcılara ait verilerin yanlış kişilerin erişimine neden olabilir. Yanlış yapılandırılmış izinler veya kullanıcı rolleri, yetkisiz kişilere kritik işlemleri gerçekleştirme veya hassas verilere erişim imkânı verebilir [43]. Bu da veri gizliliği ve güvenliği açısından büyük bir risk teşkil etmektedir.

Güvenlik İzleme ve Olay Yönetimi: Güvenlik izleme ve olay yönetimi mekanizmalarının eksik olduğu durumlarda, saldırılar fark edilmeyebilir veya zamanında müdahale edilemeyebilir. Bu da saldırıların etkilerini arttırabilmektedir. Bu nedenle, HOY hizmetleri sağlayan firmaların, etkin güvenlik izleme ve olay yönetimi süreçlerini uygulamaları ve güncel tehditlere karşı sürekli olarak izleme yapmaları önemlidir [44]. Ayrıca, güvenlik olaylarını hızlı bir şekilde tespit edebilmek için otomatik uyarı sistemleri, güvenlik bilgi ve olay yönetim araçları ve güvenlik ekibinin proaktif bir yaklaşım sergilemesi gibi önlemler almak da oldukça önemlidir [40].

Çoklu Kiracılık: HOY modelinde, çoklu kiracılık önemli bir sorun olarak ortaya çıkmaktadır. Çoklu kiracılık, aynı uygulamanın birden fazla müşteri veya kiracı tarafından paylaşıldığı bir ortamı ifade eder. Bu durumda, müşteriler aynı uygulama örneğini kullanırken, veriler ve kaynaklar birbirinden izole edilmeye çalışılsa da güvenlik konusunda büyük bir endişe doğmaktadır. Çoklu kiracılık, veri gizliliği, güvenlik izolasyonu ve ayrıcalıklı erişim kontrolleri gibi konularda dikkatli bir yaklaşım gerektirir [45]. Sağlam bir çoklu kiracılık mimarisi oluşturmak

için, kiracıların birbirlerinin verilerine ve iş yüklerine erişimini sınırlamak ve güvenlik çerçevesini oluşturmak zorunludur. Aksi takdirde, bir kiracının güvenlik açığı, diğer kiracıları ve uygulama alt yapısını tehlikeye atabilmektedir [40]. Dolayısıyla, çoklu kiracılıkta güvenlik, ciddi bir sorun ve dikkat gerektiren bir konudur.

2.3.4. Bulut Hizmetlerinde Güvenlik: HOA, HOP, HOY Farkları

HOA, HOP ve HOY hizmetlerinin farklı özellikleri, beraberinde farklı güvenlik sorunlarını getirebilir. Örneğin, HOA hizmetinde fiziksel ve sanal altyapının güvenliği önemlidir. Eğer HOY sağlayıcısının altyapısında bir güvenlik açığı varsa, bu diğer hizmet modellerinde çalışan uygulamaların güvenliğini etkileyebilir. Aynı şekilde, HOP ve HOY hizmetlerindeki yazılım güvenliği veya kimlik doğrulama sorunları da kullanıcıların veri güvenliğini riske atabilir [40].

HOP hizmetlerinde, kullanıcılar uygulamalarını geliştirme ve dağıtma süreçlerinde bir platform kullanır. Uygulama katmanı güvenliği önemli bir sorun haline gelir. Zayıf yazılım güvenliği, hatalı yapılandırma ve yetkisiz erişim kontrolleri gibi sorunlar, kötü niyetli kullanıcıların veya saldırganların uygulamaları hedef almasına neden olabilir.

HOY hizmetlerinde ise kullanıcılar uygulamaları ve verileri üzerinde çalışır. Güvenlik sorunları genellikle veri güvenliği, kimlik doğrulama ve erişim kontrolleri, güvenlik izleme ve hizmet kesintileri gibi alanları kapsar. Kullanıcılar, veri güvenliği için uygun şifreleme yöntemlerini kullanmalı, güçlü kimlik doğrulama ve erişim kontrolleri uygulamalıdır. Ayrıca, hizmet sağlayıcının güvenlik önlemlerini değerlendirmek ve hizmet kesintileri durumunda iş sürekliliği planlaması yapmak önemlidir.

Bu şekilde, HOP, HOA ve HOY hizmetlerinin farklı yapıları ve sorumluluk alanları, farklı güvenlik sorunlarını beraberinde getirir. Ancak bu hizmet modelleri arasında birbirini tamamlayan bir ilişki vardır. HOP, uygulama geliştirme ve dağıtma platformunu sağlar, HOA altta yatan altyapıyı ve HOY ise kullanıcıya hizmet olarak uygulamaları sunar. Bu nedenle, her bir hizmet modelinin güvenlik sorunları birbirleriyle ilişkilidir ve bir modelde yaşanan bir güvenlik sorunu diğer modelleri de etkileyebilir [46].

2.4. Bulutta Yaşanan Güvenlik Sorunlarına Karşı Alınan Önlemler

Bulut ortamında güvenlik, dışarıdan temin edilen verilerin risk analiziyle başlar. Bu analiz, verilerin kötüye kullanılması yerine tüm olası kullanımları göz önünde bulundurarak yapılmalıdır. Verilerin sınıflandırılması, risklere odaklanmayı ve daha önemli verilere öncelik verilmesini sağlar. Bulut sağlayıcıları, güvenlik önlemleriyle birlikte verilerin korunmasını sağlamak için fiziksel güvenlik, şifreleme, erişim kontrolleri ve ağ güvenliği gibi önlemler alır. Bununla birlikte, bulut kullanıcıları da kendi sorumlulukları çerçevesinde güvenlik önlemlerini uygulamalı ve verilerini

korumak için doğru yapılandırmaları sağlamalıdır [47]. Böylece, bu güvenlik ortamını sağlamak, yeni devrim niteliğindeki bulut teknolojisinin ilerlemesine büyük katkı sağlayacaktır.

Bulut bilişimdeki güvenlik sorunlarına karşı alınan önlemlerle ilgili birçok çalışma yapılmaktadır. Akademik araştırmalar, endüstri standartları ve çeşitli raporlar, bulut ortamında güvenliği artırmak için önemli öneriler sunmaktadır. Bu çalışmalar, güvenlik açıklarını tespit etmek, saldırıları önlemek ve hızlı bir şekilde yanıt verebilmek amacıyla bir dizi önlemi kapsar. Tüm bu araştırmalar ve alınan önlemler, bulut bilişimde güvenlik sorunlarıyla başa çıkmak için sürekli bir çaba ve dikkatin gerektiğini vurgulamaktadır. Hem bulut sağlayıcıları hem de kullanıcılar, güvenlik önlemlerini sürekli olarak güncellemeli ve geliştirmelidir. Böylece veriler ve hizmetler güvende olabilir. Yapılan araştırmalar sonucunda literatürde bulut güvenlik sorunlarına karşı alınan önlemler derlenip Tablo 2.1’de verilmiştir.

Tablo 2.1. Bulutta Yaşanan Güvenlik Sorunları ve Alınan Önlemler

Güvenlik Sorunu	Alınan Önlemler
Veri Sızıntısı/Veri İhlali	Veri Şifreleme [48] Erişim Kontrolü [49] Güçlü Kimlik Doğrulama [50] Veri Sızıntısı İçin İleri Tehdit Tespit Sistemleri [51]
Hesap Hırsızlığı	Güçlü Kimlik Doğrulama [50,33] Çok Faktörlü Kimlik Doğrulama [52] Kullanıcı Eğitimi ve Farkındalığı [53] Hesap İzleme ve Etkinlik Kayıtları [54] Hesap Kurtarma Mekanizmaları [55]
Hizmet Kesintileri	İzleme ve Uyarı Sistemleri [56] Risk Değerlendirmesi ve Planlama [57]
Kötü Amaçlı Yazılımlar	Güvenlik Yazılımlarının Kullanılması [46]
Yetkilendirme Hataları	Doğru Yetkilendirme Politikalarının Oluşturulması Ve Uygulanması [46] İhtiyaç Temelli Erişim Kontrolleri [49]
Zayıf Ağ Güvenliği	Ağ Trafiklerinin İzlenmesi ve Sızma Önlemlerinin Alınması [59]
Paylaşılan Kaynaklar	İzolasyon [60]
Sanallaştırma	Sanal Makine Güvenliği [61] Sanal Ağ Güvenliği [40]
Çoklu Kiracılık	Sözleşmeler ve Hizmet Seviyesi Anlaşmaları [46] Veri ve Kaynak İzolasyonu [62]

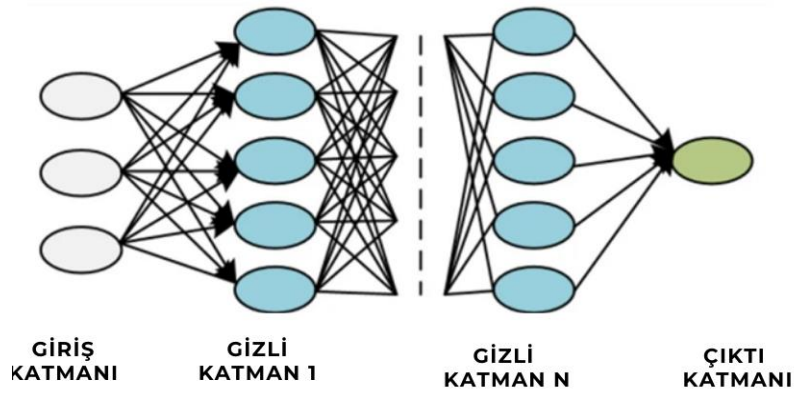
3. DERİN ÖĞRENME

Yapay sinir ağlarının gelişimi, çok katmanlı mimarilerin ortaya çıkmasına öncülük etmiştir. Bu gelişimin devamında Derin Sinir Ağları (DSA) ve Derin Öğrenme (DÖ) birçok alanda kullanılmaya başlayan bir yöntem olmuştur. DÖ’de geçen "derin" terimi, çok katmanlı sinir ağı yapısına sahip olmasından dolayı kullanılmaktadır.

Geleneksel makine öğrenimi tekniklerinde, özellik çıkarıcılar insanlar tarafından manuel olarak tasarlanır ve belirli bir problem veya veri kümesi için özelleştirilir. Özellikler, uzmanların alan bilgisi ve deneyimine dayalı olarak seçilip oluşturulur. Ancak bu yöntem, büyük veri setleri ve karmaşık problemlerle karşılaşıldığında sınırlamalar getirir. İnsanların el ile özellikleri tanımlaması ve ayarlaması zaman alıcı ve zorlu bir süreç olabilir ve bazen veri setinin karmaşıklığını tam olarak yansıtamayabilir [63].

Derin öğrenme bu sınırları aşmayı hedefleyen bir yaklaşımdır. Otomatik olarak veri içindeki temsil özelliklerini öğrenen çok katmanlı yapıları içerir. Bu metodun temelinde, veri setindeki desenlerin keşfedilmesi ve temsil edilmesi için insan müdahalesine gerek duyulmaz. Yapay sinir ağları kullanılarak derin öğrenme modelleri oluşturulur ve büyük ölçekli veri setleri üzerinde eğitilir. Bu modeller, veriyi daha yüksek soyutlama seviyelerinde temsil ederek ve otomatik olarak özellikleri belirleyerek karmaşık ve doğal veri setlerindeki ilişkileri daha etkin bir şekilde öğrenirler [63, 64].

DSA’lar katmanlar halinde bir araya gelmiş nöronlardan oluşmaktadır. Nöronların buradaki işlevi karar vermektir. Aldıkları bilgileri bir takım matematiksel işlemlerden geçirerek elde ettiği sonucu bağlantılı sonraki nörona aktarmaktadır. Şekil 3.1’de derin sinir ağına ait mimariye yer verilmektedir.



Şekil 3.1. Derin Sinir Ağı Mimarisi [65]

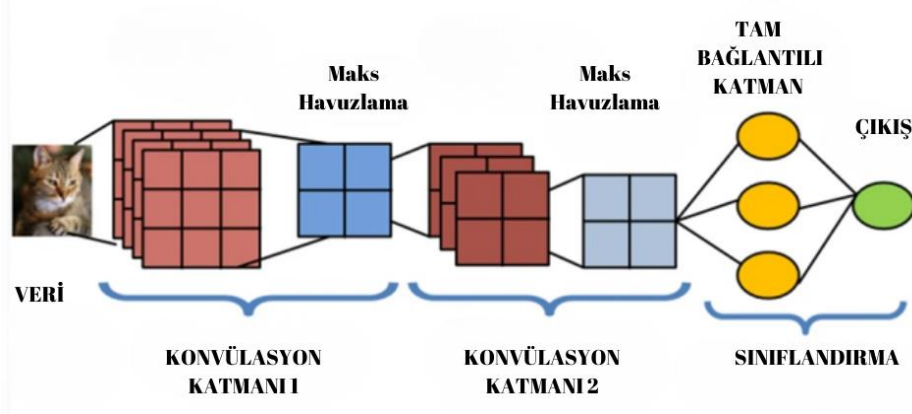
Bir nöronun işlevi, verilen girdiye dayalı olarak bilgiyi almak, işlemek ve çıktı üretmektir. Bu, girdiyi ağırlık değişkeniyle çarparak ve sapma değişkeniyle toplayarak sonucu elde etmek suretiyle gerçekleştirilir. Ardından, elde edilen sonuç bir aktivasyon fonksiyonundan geçirilerek çıktı oluşturulur. Nöronun görevi burada sona erer. Üretilen çıktı, bağlı olduğu nörona iletilir ve işlem katmanları içerisinde devam eder. Öğrenme süreci, ağırlık ve sapma değişkenlerinin algoritma tarafından sürekli olarak ayarlanması yoluyla gerçekleştirilir [66]. Denklem 3.1’de bir nöronun çıktısını belirleyen aktivasyon fonksiyonunun matematiksel denklemi verilmiştir.

$$y = \text{aktivasyon}(\sum(\text{ağırlık} * \text{giriş}) + \text{eşik}) \quad (3.1)$$

3.1. Evrimsel Sinir Ağları

ESA, derin öğrenme temelli bir sinir ağı olup birçok problem için yaygın olarak kullanılan bir modeldir. Özellikle görüntü tanıma ve sınıflandırma gibi görsel işleme problemlerinde başarılı sonuçlar vermektedir. ESA’ların etkinliği, verideki desenleri otomatik olarak öğrenme ve karmaşık ilişkileri doğru bir şekilde modelleme yeteneklerinden kaynaklanır. Büyük veri setleri üzerinde eğitildiklerinde, problemin çözümüne yönelik iyi sonuçlar elde edilebilir [67].

ESA’lar veri üzerinde konvolüsyon işlemi ardından elde edilen özellik haritalarını havuzlama işlemi ve son olarak aktivasyon fonksiyonlarıyla işleyen katmanlardan oluşmaktadır. Konvolüsyon işlemi, verinin üzerinde önceden belirlenmiş filtrelerin kaydırılması ve çaprazlama işlemi yapmasıyla gerçekleşir. Bu sayede görüntüdeki özelliklerin lokal bağımlılıklarını yakalayıp, çeşitli özellik haritaları elde edilebilir. Daha sonra havuzlama katmanı özellik haritalarını küçültür ve böylece hesaplama yükü azalır [68]. Elde edilen özellik haritalarının boyutu küçültülürken maksimum havuzlama ve ortalama havuzlama gibi yöntemler kullanılarak, önemli özelliklerin korunması hedeflenir [67]. ESA’ların son katmanlarında genellikle tam bağlantılı katmanlar yer alır. Bu katmanlar, özellik haritalarını kullanarak sınıflandırma, tespit veya diğer görevleri gerçekleştirir. Şekil 3.2’de bu katmanlar gösterilmiştir.



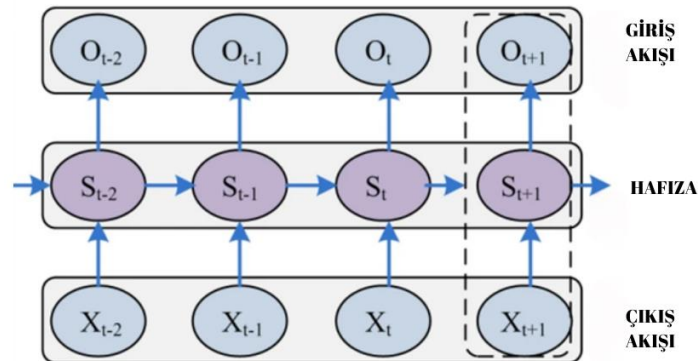
Şekil 3.2. Evrimsel Sinir Ağı Yapısı [65]

3.2. Tekrarlayıcı Sinir Ağı

TSA, sıralı verilerin işlenmesi ve zaman bağımlı ilişkilerin modellenmesi için özel olarak tasarlanmış derin öğrenme tabanlı bir yapay sinir ağıdır. TSA ağında çıkış bir sonraki adımı beslediği için döngüsel bir yapıya sahiptir. Bu sayede TSA'lar geçmiş bilgiyi hafızada tutup gelecekteki adımlarla bu bilgiyi kullanır. Bu özelliğinden dolayı zaman serisi verilerini ve diğer sıralı veri türlerini etkili bir şekilde işleyebilir [69].

TSA'ların çalışma yapısında, mevcut giriş ve önceki adımdan gelen gizli durum olmak üzere iki ana bileşen kullanılır. Gizli durum, geçmiş bilgiyi temsil eder bu nedenle TSA'nın belleği olarak düşünülebilir. Yeni gelen bilgiyle her adımda gizli durum güncellenir ve gelecekteki adımlarda kullanılmak üzere saklanır. Şekil 3.3'te TSA'nın çalışma prensibi gösterilmiştir.

Yapılan çalışmalar sonucunda basit TSA'ların kaybolan ve patlayan gradyan sorunları nedeniyle uzun süreli bağımlılıkları iyi modelleyemediği görülmüştür. Bu sorunların üstesinden gelmek için daha gelişmiş TSA varyantları bulunmaktadır [70].



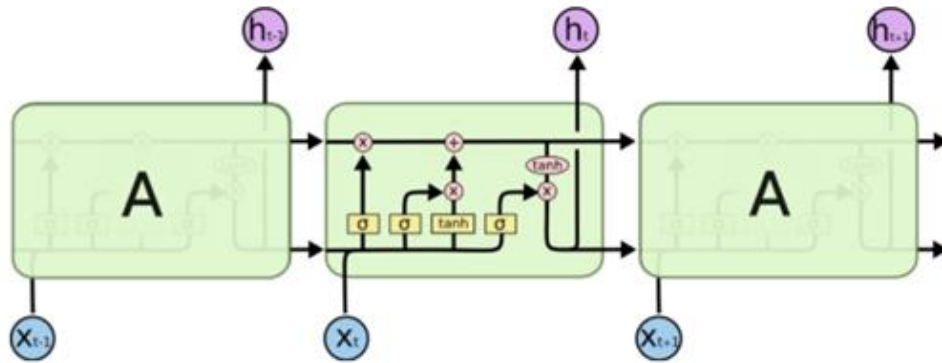
Şekil 3.3. Tekrarlayıcı Sinir Ağı Yapısı [65]

3.2.1. Uzun Kısa Süreli Bellek

UKSB, TSA ailesine ait bir hücre tipidir ve özellikle zaman serisi verileri, doğal dil işleme ve benzeri alanlarda başarılı bir şekilde kullanılan bir derin öğrenme modelidir. UKSB'ler TSA'larda kaybolan ve patlayan gradyan sorunlarına çözüm getirmektedir. Bu sayede, uzun süreli bağımlılıkları daha etkili bir şekilde modelleyebilmektedir.

UKSB hücresi, bir hücre durumu ve unutma kapısı, giriş kapısı ve çıkış kapısı olmak üzere üç ana kapıdan oluşan bir yapıya sahiptir. Bu kapılar, hücre durumunun nasıl güncelleneceğini ve hangi bilgilerin aktarılacağını kontrol etmektedir. Unutma kapısı, geçmiş bilginin ne kadarının tutulacağını belirlerken, giriş kapısı mevcut giriş ve önceki gizli durum ile birlikte hangi bilgilerin hücre durumuna ekleneceğini belirlemektedir. Çıkış kapısı ise hücre durumundan hangi bilgilerin çıkış olarak kullanılacağını belirlemektedir [71]. Şekil 3.4'te bir hücreli UKSB bellek bloğu görülmektedir.

UKSB'nin önemli bir özelliği, hücre durumunda uzun vadeli bağımlılıkları koruyabilme yeteneğine sahip olmasıdır. Bu, bir girdinin etkisinin uzak geçmişe kadar uzanabileceği ve UKSB'nin bu bağımlılıkları etkili bir şekilde hatırlayabilmesini sağlar. UKSB, derin öğrenme alanında büyük bir ilgi görmüş ve birçok araştırmacı tarafından kullanılan güçlü bir yapay sinir ağı mekanizmasıdır. Bu model, karmaşık veri yapılarındaki desenleri ve ilişkileri keşfetmek için etkili bir şekilde kullanılabilir.



Şekil 3.4. Tek Hücreli LSTM [72]

3.3. Derin Öğrenme Yöntemlerinin Saldırı Tespit Sistemlerinde Kullanılması

Saldırı tespit sistemleri, ağ veya bilgisayar sistemlerindeki olası saldırıları belirlemek ve engellemek için kullanılan yazılım ve donanım bileşenlerinden oluşan bir güvenlik önlemidir. Bu sistemler, ağ trafiğini gözlemleyerek, analiz ederek ve anormal faaliyetleri veya saldırı işaretlerini tespit etmeye çalışır.

Son yıllarda, saldırı tespit sistemlerinde derin öğrenme yöntemi önemli bir rol oynamaktadır. Derin öğrenme, karmaşık veri kümelerini analiz etmek ve desenleri tespit etmek için çok katmanlı

yapılara sahip yapay sinir ağlarını kullanır. Derin öğrenme, saldırı tespiti için ağ trafiği, günlük kayıtları ve diğer güvenlik verileri gibi geniş ve karmaşık veri setlerini etkili bir şekilde analiz etmek amacıyla kullanılabilir.

3.3.1. Anomali Tespiti

Anomali tespiti, normal ağ trafiği veya sistem davranışlarının izlenerek, bu normal davranıştan sapmaları tespit etme yeteneğini ifade etmektedir. Anomali tespiti için derin öğrenme, ağ trafiği, kullanıcı davranışı, sistem kayıtları veya diğer güvenlik verileri gibi kaynakları kullanır. Derin öğrenme, büyük veri kümelerini analiz ederek sistemin normal çalışma durumunu ve davranışını modelleyebilmektedir [73]. Ağ trafiği veya sistem davranışına ait veri kümesi büyük hacimli olması nedeniyle bu büyük veriler üzerinde eğitilen bir derin öğrenme modeli, normal davranışı öğrenebilir ve bu temele dayanarak normal olmayan davranışları belirlemek için gelen verileri analiz edebilir.

Normal davranıştan sapmalar, saldırıların veya diğer zararlı etkinliklerin göstergeleri olabilir. Örneğin, bir ağdaki normal trafiğe alışkın olan bir derin öğrenme modeli, anormal bir ağ trafiği modeli tanımlayabilir ve saldırı girişimlerini tespit edebilir. Bu tür bir model, bilinen saldırı imzalarına veya tanımlanmış saldırı kalıplarına ihtiyaç duymaz; bunun yerine, normal davranıştan sapmaları otomatik olarak tespit etmeye çalışır [74].

Derin öğrenme tabanlı anomali tespiti, bilinmeyen veya gelişmiş saldırı türlerini de tespit edebilir. Çünkü model, normal davranışı anlamak için geniş bir veri kümesiyle eğitilir ve bu sayede önceki bilgiye dayanmaksızın anormallikleri belirleyebilir. Ancak, derin öğrenme tabanlı anomali tespiti bazı zorluklarla karşılaşabilir. Veri setlerinin büyüklüğü ve karmaşıklığı, modelin eğitimi için yeterli veri ve hesaplama kaynaklarının gerekliliğini artırır. Bu nedenle veri setlerinin doğru bir şekilde eğitilmesi ve modelin hassaslığının ayarlanması gerekmektedir [75].

3.3.2. İmza Tabanlı Tespitin Güçlendirilmesi

İmza tabanlı saldırı tespit sistemleri, önceden bilinen saldırı imzalarını kullanarak saldırıları tespit etmeye çalışmaktadır. Ancak, bu sistemlerin dezavantajı, yeni veya değiştirilmiş saldırı türlerini tanıyamamasıdır. Bu sorun derin öğrenme kullanılarak giderilmeye çalışılmaktadır [76].

Derin öğrenme algoritmaları, büyük veri setlerini analiz ederek saldırı imzalarını tespit etmek için daha etkili ve hassas bir şekilde öğrenebilir. Bir derin öğrenme modeli, geniş bir veri kümesindeki saldırı örneklerini ve normal ağ trafiğini öğrenerek, bu saldırıları otomatik olarak tanımlamak için kalıpları öğrenebilme yeteneğine sahiptir.

Derin öğrenme, imza tabanlı saldırı tespit sistemlerini güçlendirmek için kullanılabilir çünkü bir derin öğrenme modeli, geleneksel yöntemlerden farklı olarak saldırı imzalarını doğrudan belirlemek yerine, saldırıların temel özelliklerini kendisi keşfedebilir. Bu, yeni veya değiştirilmiş saldırı türlerini tespit etme yeteneğini artırır [77].

Bununla birlikte, derin öğrenme modellerinin eğitimi için yeterli ve temsilci bir veri kümesine ihtiyaç vardır. Büyük veri setleri, modelin çeşitli saldırı tiplerini ve normal davranışı anlamasına yardımcı olabilir. Ayrıca, modelin doğruluğunu ve güvenilirliğini değerlendirmek için uygun doğrulama ve test süreçleri gereklidir.

3.3.3. Veri Madenciliği ve Özellik Çıkarımı

Veri madenciliği ve özellik çıkarımı, derin öğrenme yöntemiyle saldırı tespiti için kullanılan verilerden anlamlı özellikleri tanımlamayı içerir. Bu, saldırıları tespit etmek ve yanlış pozitif oranını azaltmak için daha iyi bir temsil sağlayabilir.

Derin öğrenme, veri madenciliği tekniklerini kullanarak, saldırıları tespit etmek için önemli özelliklerin çıkarılmasını sağlayabilir. Bu özellikler, saldırılarla ilgili belirli davranış kalıplarını veya istatistiksel anormallikleri temsil edebilir. Örneğin, bir derin öğrenme modeli, ağ trafiğindeki belirli paket yapıları, protokol davranışları veya bağlantı süreleri gibi özellikleri tanımlayabilir. Bu özellikler, saldırıları tespit etmek için daha iyi bir temsil sağlayabilir. Derin öğrenme modeli, bu özellikler üzerinde eğitildiğinde, saldırıları tespit etmek ve normal ağ trafiğinden ayırmak için daha hassas ve etkili olabilir [78].

Ayrıca, veri madenciliği ve özellik çıkarımı, yanlış pozitif oranını azaltmaya yardımcı olabilir. Yanlış pozitif, normal ağ trafiğini yanlışlıkla bir saldırı olarak tanımlayan hatalı bir alarmı ifade eder. Derin öğrenme algoritmaları, doğru ve anlamlı özelliklerin çıkarılması sayesinde yanlış pozitif oranını düşürebilir ve daha doğru saldırı tespiti sağlayabilir [79].

Sonuç olarak, derin öğrenme, saldırı tespit sistemleri için veri madenciliği ve özellik çıkarımıyla birlikte kullanıldığında, önemli özelliklerin keşfedilmesine ve saldırıları tespit etmek için daha iyi bir temsil elde edilmesine katkıda bulunabilir. Bu, saldırı tespit sistemlerinin performansını artırabilir ve yanlış alarm oranını azaltabilir.

3.3.4. Gerçek Zamanlı Saldırı Tespiti

Gerçek zamanlı saldırı tespiti, sızma tespit sistemlerinin önemli bir unsuru olup, derin öğrenme algoritmaları bu amaç için etkili bir şekilde adapte edilebilir. Gerçek zamanlı saldırı tespiti, ağ trafiğini gerçekleştirdiği anda analiz etme ve saldırıları engellemek veya hafifletmek için hızlı bir şekilde tepki verme yeteneğini ifade eder.

Derin öğrenme algoritmaları, büyük veri kümelerini hızlı bir şekilde işleme ve analiz etme konusunda başarılıdır, bu da onları gerçek zamanlı saldırı tespiti için uygun kılar. Bu algoritmalar, ağ trafiğini sürekli olarak gerçek zamanlı olarak izleyebilir ve analiz edebilir, böylece desenleri, anormallikleri veya bilinen saldırı imzalarını ortaya çıktığı anda tespit edebilir [80].

Derin sinir ağlarının gücünden yararlanarak, gerçek zamanlı saldırı tespit sistemleri tarihsel verilerden öğrenebilir ve geleneksel kural tabanlı yaklaşımlarda açıkça tanımlanmayan karmaşık saldırı kalıplarını tanıyabilir. Derin öğrenme modelleri, ağ trafiği verilerinden karmaşık özellikleri çıkarabilir ve geleneksel tespit mekanizmalarının kaçırabileceği zararlı etkinliklerin belirtilerini yakalayabilir.



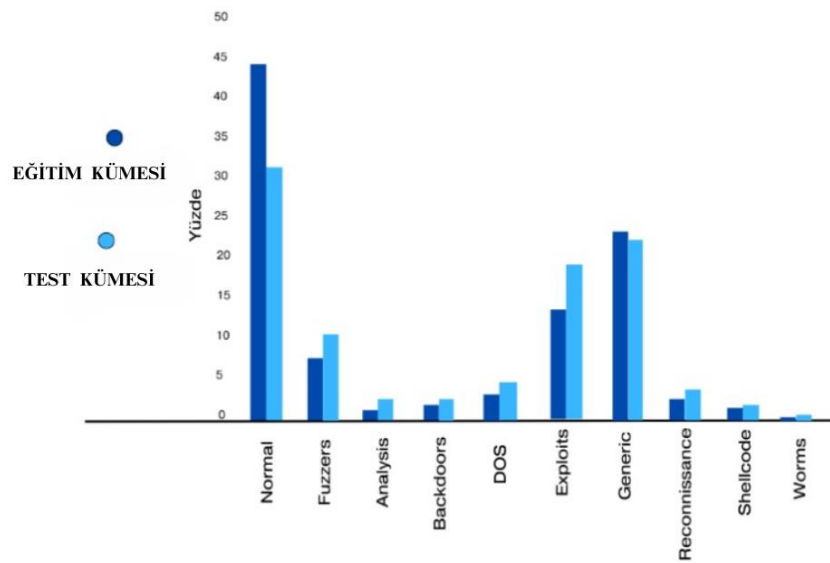
4. MATERYAL VE METOT

Bu bölümde, bulut bilişime yönelik saldırıları tespit etmek için kullanılan materyal ve yöntemler hakkında bilgi sunulmaktadır. Tez kapsamında kullanılan AWID ve UNSW-NB15 veri setleri incelenirken, bu veri setlerinin ön işleme adımları detaylı bir şekilde açıklanmaktadır. Sonrasında saldırı tespitinde kullanılan modellerin, eğitilmesi için uygulanan derin öğrenme algoritmaları ve oluşturulan hiyerarşik yapılar açıklanmaktadır.

4.1. Materyal

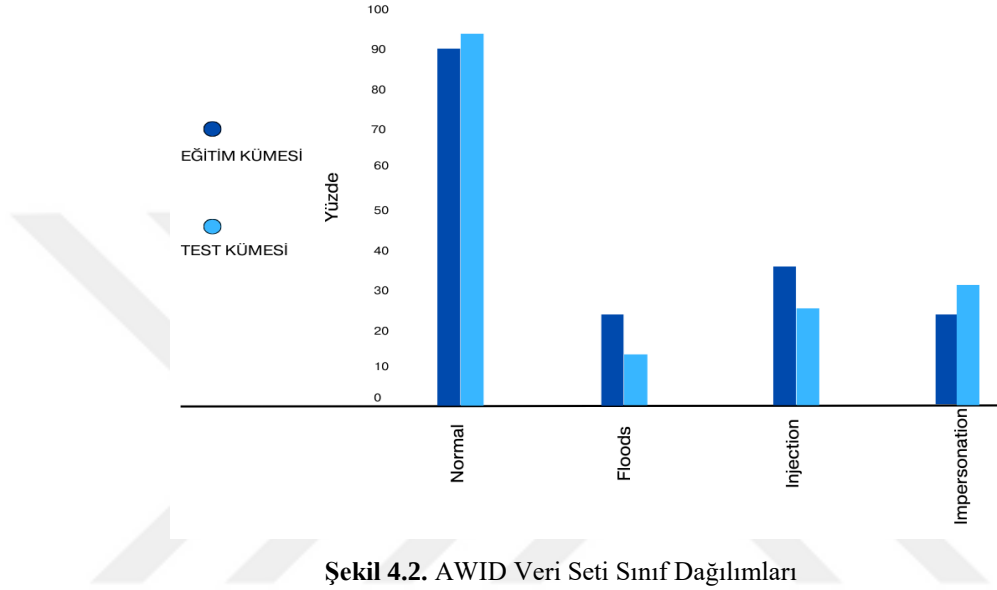
Bu tez çalışmasında, ağ izinsiz giriş veri tespiti için günümüz en güncel veri setlerinden olan UNSW-NB15 ve AWID kullanılmıştır. Bu veri setleri, siber güvenlik araştırmacıları ve güvenlik uzmanları için önemli bir rol oynamaktadır. Bu veri setlerinin kullanılması, saldırı tespiti sistemlerinin geliştirilmesine, güvenlik açıklarının tespit edilmesine ve ağların daha güvenli hale getirilmesine katkıda bulunmaktadır.

UNSW-NB15 Avustralya Siber Güvenlik Merkezi tarafından oluşturulmuştur. Bu veri kümesi için saldırı örnekleri, web sitelerine yapılan saldırılardan toplanmıştır. Örnek saldırılar daha sonra veri seti üretimi için bir laboratuvar ortamında simüle edilmiştir. Bu veri kümesinde Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode ve Worms olmak üzere 9 tür saldırı ve 49 özellik bulunmaktadır [19]. UNSW-NB15 veri kümesinin eğitim ve test verilerine ait sınıf dağılımları, Şekil 4.1'de gösterilmektedir.



Şekil 4.1. UNSW-NB15 Veri Seti Sınıf Dağılımları

Diğer bir veri seti Aegean Wi-Fi Intrusion Dataset (AWID) kablosuz ağlarda izinsiz giriş tespit deneyleri için güvenilir bir test ortamıdır. AWID veri seti, çeşitli Wi-Fi ağlarında gerçekleştirilen saldırıları ve normal ağ trafiğini içeren geniş bir veri koleksiyonudur. Bu veri setinde her kayıt, kaydın normal mi yoksa bir saldırı sırasında iletilmiş mi olduğunu gösteren sınıf özelliği dâhil 155 öznitelik içerir [81]. Şekil 4.2’de bu veri setine ait eğitim ve test verilerinin sınıf dağılımı gösterilmektedir.



Şekil 4.2. AWID Veri Seti Sınıf Dağılımları

Çalışma kapsamında bulutun katmanlı yapısı göz önünde bulundurularak, fiziksel saldırılara odaklanmak için UNSW-NB15 veri seti, 802.11 saldırılarına odaklanmak için AWID veri seti seçilmiştir.

4.2. Metot

Saldırı tespit sistemlerinde daha karmaşık saldırı modellerini tespit etmek, anormal davranışları tespit etmek ve gerçek zamanlı tepkiler vermek gibi avantajlar sunduğu için derin öğrenme alanında birçok çalışma bulunmaktadır. Bu tez çalışması kapsamında bulut güvenliği için derin öğrenme sinir ağları kullanılarak saldırı tespit sistemlerinin güvenlik seviyelerini artırmak ve gelişmiş saldırı tekniklerine karşı daha iyi koruma sağlamaya çalışılmıştır.

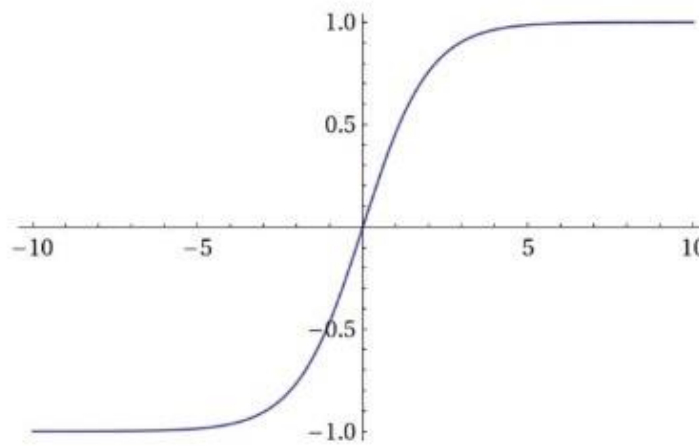
Çalışmada birçok alanda önemli başarılar elde edilen ESA ve TSA sınıfına ait UKSB sinir ağları kullanılarak iki farklı model geliştirilmiştir. Paralel ESA-UKSB olarak tanımladığımız ilk modelde, giriş verileri ESA ve UKSB sinir ağları üzerinde bağımsız olarak çalışmakta ve çıktıları paralel bir şekilde birleştirilmektedir. Hiyerarşik ESA-UKSB tanımladığımız ikinci modelde ise UKSB, ESA tarafından öğrenilen giriş verilerinin özelliklerini öğrenmek için kullanılmaktadır. Bu iki model yukarıda adı geçen veri setleri kullanılarak eğitilip test edilmiştir.

4.2.1. Softmax Aktivasyon Fonksiyonu

Softmax, genellikle çok sınıflı sınıflandırma problemlerinde kullanılan bir aktivasyon fonksiyonudur [82]. İsmi, fonksiyonun çıktıları olasılık dağılımına dönüştürmesinden alır. Denklem 4.1’de softmax aktivasyon fonksiyonuna ait matematiksel ifade verilmiştir.

$$y_i = \frac{e^{z_i}}{\sum_{i=0}^n e^{z_i}} \quad (4.1)$$

Bu tez çalışmasında veri setlerinde çoklu sınıf bulunduğu için bu sınıflandırıcının kullanılması tercih edildi. Softmax fonksiyonu, bir vektörün elemanlarını 0 ile 1 arasında ve toplamının 1’e eşit olduğu bir olasılık dağılımına dönüştürür. Bu, çıktıların sınıf olasılıklarını temsil etmesini sağlar. Softmax fonksiyonu, en yüksek olasılığa sahip sınıfı seçmek için sıklıkla kullanılır [83]. Şekil 4.3’te softmax fonksiyonuna ait grafik verilmiştir.

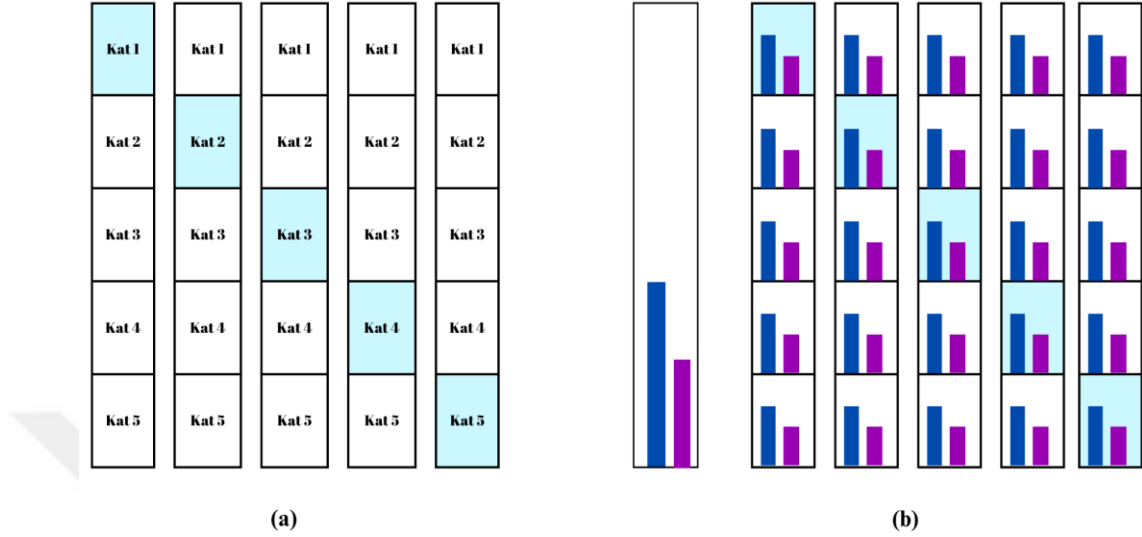


Şekil 4.3. Softmax Fonksiyonu [82]

4.2.2. Çapraz Doğrulama Yöntemi

Çapraz doğrulama, bir makine öğrenimi modelinin genel performansını değerlendirmek ve aynı zamanda aşırı uydurmayı tespit etmek için kullanılan bir tekniktir [84]. Bu çalışmada çapraz doğrulama yöntemlerinden biri olan Katmanlı Çapraz Doğrulama kullanılmaktadır. Bu yöntem dengesiz sınıf dağılımına sahip veri kümelerinde performansının değerlendirilmesi için tasarlanmıştır. Çapraz doğrulama, veri kümesini k eşit parçaya böler ve ardından modelinizi k kez eğitip değerlendirmenizi sağlar. Katmanlı Çapraz Doğrulama bu işlemi sınıflara ayrılmış örnekler dikkate alarak gerçekleştirir, böylece her katmanın tüm sınıfları adil bir şekilde temsil ettiğinden

emin olur [85]. Şekil 4.4'te 5 katlı çapraz doğrulama örneği ve 5 katlı katmanlı çapraz doğrulama örneği gösterilmiştir.



Şekil 4.4. 5 Kat Çapraz Doğrulama Örneği (a), 5 Katlı Katmanlı Çapraz Doğrulama Örneği (b)

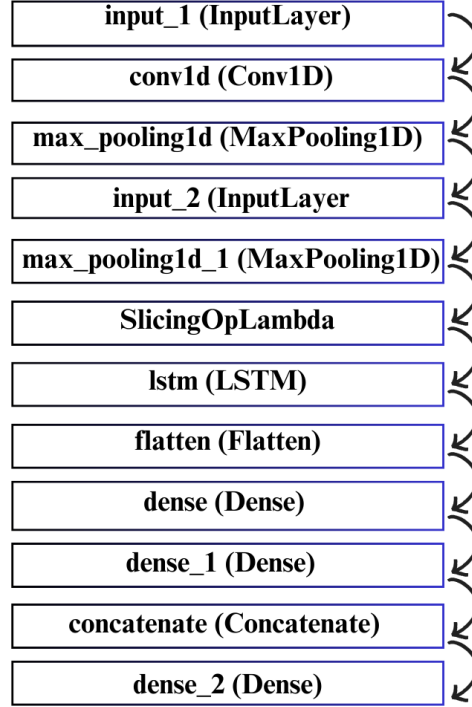
4.2.3. Paralel ESA-UKSB Tabanlı İzinsiz Giriş Modeli

Önerilen paralel mimari, ESA ve UKSB'nin ayrı bir şekilde çalıştırılıp çıktılarının birleştirildiği bir yapıdır. Bu yöntemde, veri seti hem ESA hem de UKSB'ye ayrı ayrı giriş olarak verilir. Her bir ağ, kendi öğrenme mekanizmasını kullanarak girdi verileri üzerinde işlem yapar [86].

ESA, verilerdeki yerel desenleri tanımlamak ve özellikleri çıkarmak amacıyla kullanılan bir modeldir. ESA, konvolüsyon ve havuzlama katmanlarından oluşur. Konvolüsyon katmanları, filtrelerle dayalı olarak girdi verilerinde farklı özellikleri tespit eder. Havuzlama katmanları ise veri boyutunu küçültür ve önemli özellikleri vurgular. Bu sayede ESA, verilerdeki yerel kalıpları öğrenir.

UKSB ise sıralı verilerdeki uzun vadeli bağımlılıkları yakalamak için kullanılır. UKSB, hafıza hücreleri ve giriş, çıkış ve unutma kapılarından oluşan bir yapısı vardır. Hafıza hücreleri, geçmiş bilgileri saklamak ve güncel bilgilerle birleştirerek uzun vadeli bağımlılıkları öğrenmek için kullanılır. Bu sayede UKSB, sıralı verilerdeki zaman bağımlılıklarını ve ilişkileri modelleyebilir. Paralel bir mimaride, her bir ağın çıktıları daha sonra birleştirilerek tamamen bağlı bir katmana geçirilir. Bu katman, ESA ve UKSB'nin çıktılarından elde edilen özellikleri bir araya getirir ve birleştirir. Bu sayede, her bir ağın güçlü yönlerini kullanarak zaman serisi verilerinin özelliklerini daha kapsamlı bir şekilde öğrenmek mümkün olur. Birleştirme işlemi, özellik vektörlerinin veya sinyallerin birleştirilmesi, ortalama veya maksimum değerlerin alınması gibi yöntemlerle

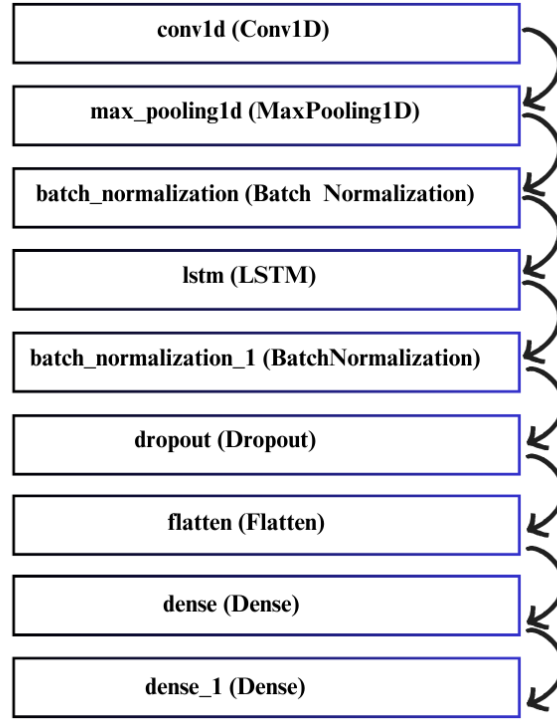
gerçekleştirilebilir. Şekil 4.5'te paralel ESA-UKSB tabanlı modele ait oluşturulan katmanlar gösterilmektedir.



Şekil 4.5. Paralel ESA-UKSB Tabanlı Modele Ait Katmanlar

4.2.4. Hiyerarşik ESA-UKSB Tabanlı İzinsiz Giriş Tespit Modeli

ESA tek başına sıralı verilerdeki zaman bağımlılıklarını yakalamakta sınırlıdır. Bu noktada, ESA'nın çıktılarını UKSB'nin girişi olarak kullanmak önemlidir [19]. ESA, farklı filtrelerin uygulanması ve özellik haritalarının oluşturulması yoluyla veri üzerinde yerel özelliklerin algılanmasını sağlar. Bu modelde çıktılar, sıralı verilerdeki uzun vadeli bağımlılıkları yakalamak için UKSB'ye giriş olarak verilir. UKSB, sıralı verilerdeki uzun vadeli bağımlılıkları modellemek için hafıza hücreleriyle çalışır. ESA tarafından öğrenilen özellikleri kullanarak, UKSB, verinin zaman içindeki değişimlerini ve bağımlılıklarını daha iyi anlayabilir. Şekil 4.6'da hiyerarşik ESA-UKSB tabanlı modele ait oluşturulan katmanlar gösterilmektedir.



Şekil 4.6. Hiyerarşik ESA-UKSB Tabanlı Modele Ait Katmanlar

4.3. Performans Değerlendirme

Sınıflandırma modellerinin performansını değerlendirmek için çeşitli performans metrikleri kullanılmaktadır. Bu metrikler, modelin ne kadar iyi çalıştığını anlamak ve modelin sınıfları doğru bir şekilde tahmin edip etmediğini değerlendirmek için önemlidir. Aşağıda oluşturulan modellerin performansı değerlendirmek için kullanılan bazı performans metrikleri tanımlanmaktadır.

Doğruluk: Doğruluk sınıflandırma problemlerinde kullanılan bir değerlendirme metriğidir. Doğru sınıflandırılan örneklerin toplam örnek sayısına oranını temsil eder. Formülü 4.2’de verilmiştir.

Aşağıda geçen DP (Doğru Pozitif), doğru pozitif sınıflandırmaların sayısını, DN (Doğru Negatif), doğru negatif sınıflandırmaların sayısını, YP (Yanlış Pozitif), yanlış pozitif sınıflandırmaların sayısını YN (Yanlış Negatif), yanlış negatif sınıflandırmaların sayısını ifade etmektedir [87,88].

$$Doğruluk = \frac{DP+DN}{DP+DN+YP+YN} \quad (4.1)$$

Hassasiyet: Hassasiyet, doğru pozitif sınıflandırmaların toplam pozitif sınıflandırmalara oranını temsil eder. Bu değer yanlış pozitiflerin sayısını azaltmayı hedefler. Yani, bir sınıfı tahmin ettiğinde ne kadar doğru olduğunu ölçer. Yüksek bir hassasiyet değeri, yanlış pozitiflerin az

olduğunu gösterir ve modelin tahminlerinin güvenilir olduğunu ifade eder [88]. Formülü 4.3'te verilmiştir.

$$Hassasiyet = \frac{DP}{DP+YP} \quad (4.2)$$

Duyarlılık: Duyarlılık, gerçek pozitif sınıflandırmaların tüm gerçek pozitif örneklerin oranını temsil eder. Duyarlılık, bir sınıfı ne kadar iyi yakaladığını ve kaç tane gerçek pozitif örneği kaçırmış olduğunu ölçer. Yani, gerçek pozitifleri ne kadar iyi tespit ettiğini ifade eder [87]. Yüksek bir duyarlılık değeri, modelin gerçek pozitifleri kaçırmaya olasılığının düşük olduğunu gösterir. Formülü 4.4'te verilmiştir.

$$Duyarlılık = \frac{DP}{DP+YN} \quad (4.3)$$

F1 Skor: F1 skor, hassasiyet ve duyarlılık metriklerinin harmonik ortalamasını ifade etmektedir. Bu metrik, modelin dengeli bir şekilde doğru pozitifleri yakaladığını ve yanlış pozitifleri azalttığını gösterir [88]. Formülü 4.5'te verilmiştir.

$$F1\ Skor = 2 * \frac{Hassasiyet * Duyarlilik}{Hassasiyet + Duyarlilik} \quad (4.4)$$

Karmaşıklık Matrisi: Karmaşıklık Matrisi, bir modelin sınıflandırma problemlerindeki performansını değerlendirmek için kullanılan önemli bir araçtır. Bu matris, modelin sınıf tahminlerini gerçek sınıf etiketleriyle karşılaştırarak, modelin hangi sınıfları ne kadar doğru veya yanlış tahmin ettiğini ayrıntılı bir şekilde gösterir [89].

AİK-EAA Eğrileri: AİK (Alıcı İşletim Karakteristiği) eğrisi, sınıflandırma modelinin hassasiyet ve özgüllüğünü farklı olasılık eşikleri kullanarak gösteren bir grafikdir. Bu eğri, modelin doğru sınıflandırma oranını yanlış sınıflandırma oranına karşı çizer. Her bir eşik değeri için DP ve YP hesaplanır ve bu değerler AİK eğrisinin oluşturulmasında kullanılır. EAA (AİK Eğrisi Altındaki Alan), AİK eğrisinin altındaki alanı ifade eder ve [0, 1] aralığında bir değer alır. Bu değer, modelin sınıflandırma yeteneğini ölçer. EAA değeri 1'e yaklaşıyorsa, model mükemmel bir performans gösteriyor demektir (DP yüksek, YP düşük). EAA değeri 0.5'e yaklaşıyorsa, modelin rastgele tahmin yapmasına benzer bir performansı olduğu anlamına gelir. EAA değeri 0.5'in altında ise, model ters yönde tahminlerde bulunuyor demektir [91].

Makro AİK, Mikro AİK: Makro AİK, her sınıfı ayrı ayrı ele alır ve ardından bu sınıfların performansını ortalama alır. Mikro AİK ise tüm sınıfların tahminlerinin birleştirildiği ve toplam performansın hesaplandığı bir metriktir [91]. Hangi metriğin kullanılacağı, problem bağlamına ve

sınıf dağılımına bağlıdır. Eğer her sınıfın performansı aynı derecede önemliyse, Makro AİK tercih edilebilir. Ancak sınıflar arasında dengesizlik varsa veya tüm sınıfların eşit derecede önemli olduğu düşünülüyorsa, Mikro AİK daha uygun bir seçenek olabilir. Her iki metrik de modelin çok sınıflı sınıflandırma performansını değerlendirmek için değerli araçlardır.



5. BULGULAR

İnternet kullanımının hızla artması bilgiye erişimi kolaylaştırmış ve dünya genelinde iletişimi büyük ölçüde geliştirmiştir. Bu gelişimle birlikte yeni teknolojiler ortaya çıkmaya başlamıştır. Bu teknolojilerin başında bulut bilişim kavramı gelmektedir. Bulut bilişim bireylere ve işletmelere hem kolaylık hem maliyet tasarrufu sunduğu için hızlı bir şekilde yaygınlaşmıştır. Ancak bu hızlı dijital dönüşüm aynı zamanda siber saldırıların da artmasına neden olmuştur. Bulut üzerindeki güvenlik açıkları ve zayıf noktalar, siber suçluların hassas verilere, mali kaynaklara ve hatta ulusal güvenliğe zarar verme potansiyeline sahip olduğu anlamına gelmektedir.

Bulut bilişim, hizmetleri ve kaynakları internet üzerinden sağlar. İnternet, kullanıcıların bulut hizmet sağlayıcılarına erişmesi ve bulutta depolanan verilere ulaşması için gereklidir. Ağ, bulut bilişimin temelindeki veri iletişimini sağlar ve kullanıcı cihazları ile bulut sunucuları arasında sürekli bir veri akışı gerçekleşir. Aynı şekilde, bulut hizmet sağlayıcıları, birden çok veri merkezine sahip olabilir ve bu merkezler arasında dağıtılmış bir ağ altyapısı kullanır. Bu dağıtık ağ yapısı, yüksek kullanılabilirlik, veri yedekleme ve hızlı erişim sağlama amacıyla tasarlanmıştır.

Bu altyapıda, özellikle büyük kuruluşlar ve hükümetler için kritik öneme sahip bilgilerin depolanması ve işlenmesi durumunda güvenlik kontrolünün sağlanması gerekmektedir. Bu veriler, ticari sırlar, finansal bilgiler, kişisel tanımlayıcı bilgiler ve hatta devlet sırları gibi çeşitli hassas bilgileri içerebilir. Siber saldırılar, bu bilgilere erişim sağlama, çalma veya hasara neden olma amacıyla gerçekleştirilebilir. Bu tür saldırılar, kuruluşların itibarına, gelirlerine ve hatta müşteri güvenine ciddi zararlar verebilir.

Bu tez çalışmasında, bulut güvenliğine katkı sağlamak amacıyla derin öğrenme yöntemleri kullanılarak ağdaki izinsiz girişleri tespit edilmeye çalışılmıştır. Çalışma kapsamında ESA ve UKSB sinir ağı kullanılarak iki farklı model oluşturulmuştur. ESA'lar, verilerdeki yerel kalıpları öğrenmek için güçlü bir yapıya sahiptir. Öte yandan, UKSB'ler sıralı verilerdeki uzun vadeli bağımlılıkları yakalama konusunda etkilidir. Bu nedenle, bu iki ağ türünün birleştirilmesi, daha iyi sonuçlar elde etmeyi başarmıştır ve oluşturulan modellerin performans değerlendirmeleri karşılaştırılmıştır.

5.1. UNSW-NB15 Veri Seti Kullanılarak Hiyerarşik ve Paralel ESA-UKSB Modelinin Değerlendirilmesi

Bu başlıkta hiyerarşik ve paralel ESA-UKSB tabanlı modelin UNSW-NB15 veri kümesi üzerinden aldığımız sonuçlara yer verilmektedir. Kullanılan modellere ait detaylı açıklama Bölüm 4'te yer verilmiştir. Hiyerarşik tabanlı modelde elde edilen doğruluk skoru %82,24 iken paralel tabanlı modele ait doğruluk skoru %82,89 olduğu görülmüştür. Ancak bu değer, tüm sınıfların performansını yeterince yansıtmadığı için diğer performans metriklerine de odaklanılmalıdır.

Tablo 5.1’de F1 Skor, hassasiyet ve duyarlılık metrikleri, UNSW-NB15 veri kümesi üzerinde her sınıf için hiyerarşik modele göre hesaplandığında elde edilen değerleri gösterilmektedir.

Tablo 5.1. Hiyerarşik ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (UNSW-NB15)

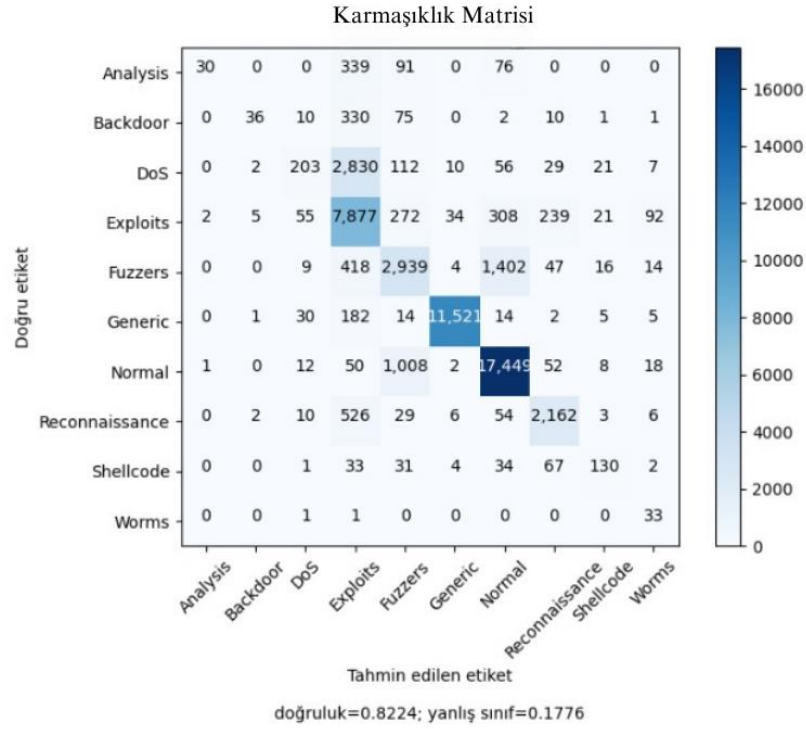
Sınıf	Hassasiyet (Hiyerarşik ESA-UKSB)	Duyarlılık (Hiyerarşik ESA-UKSB)	F1 Skor (Hiyerarşik ESA-UKSB)
Analysis	0.91	0.06	0.11
Backdoor	0.78	0.08	0.14
DoS	0.61	0.06	0.11
Exploits	0.63	0.88	0.73
Fuzzers	0.64	0.61	0.62
Generic	0.99	0.98	0.99
Normal	0.90	0.94	0.92
Reconnaissance	0.83	0.77	0.80
Shellcode	0.63	0.43	0.51
Worms	0.19	0.94	0.31

Aynı veri seti üzerinde bu metrik değerleri paralel modele göre hesaplanmıştır ve bu değerler Tablo 5.2’de sunulmaktadır.

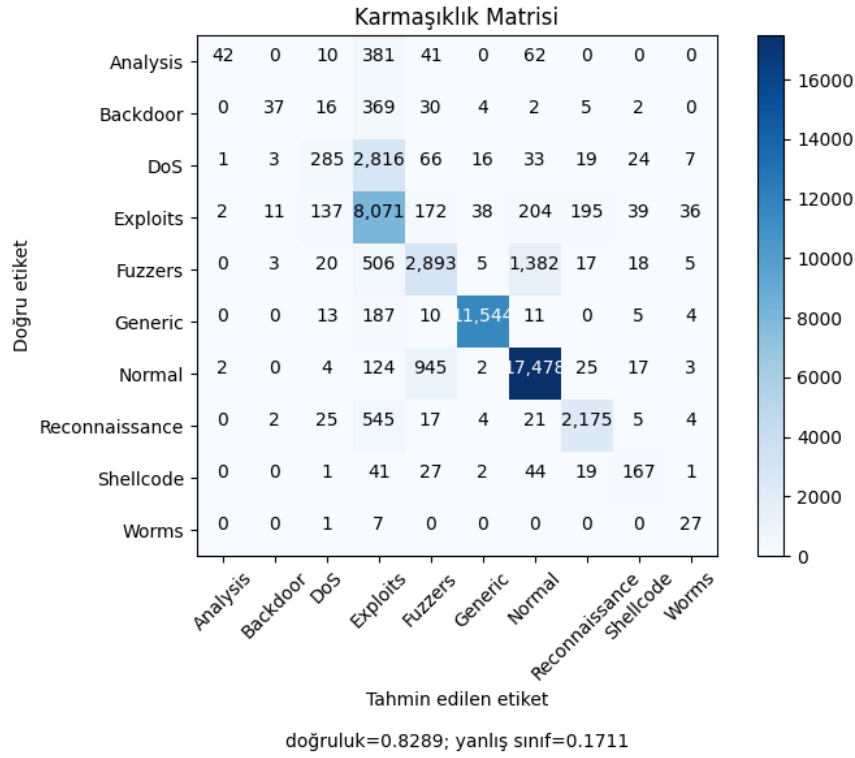
Tablo 5.2. Hiyerarşik ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (UNSW-NB15)

Sınıf	Hassasiyet (Paralel ESA-UKSB)	Duyarlılık (Paralel ESA-UKSB)	F1 Skor (Paralel ESA-UKSB)
Analysis	0.89	0.08	0.14
Backdoor	0.66	0.08	0.14
DoS	0.56	0.09	0.15
Exploits	0.62	0.91	0.74
Fuzzers	0.69	0.60	0.64
Generic	0.99	0.98	0.99
Normal	0.91	0.94	0.92
Reconnaissance	0.89	0.78	0.83
Shellcode	0.60	0.55	0.58
Worms	0.31	0.77	0.44

Veri setinde hangi sınıfların daha doğru tahmin edildiği ve hangi sınıfların karıştığını anlamak, modelin performansını değerlendirmek açısından son derece önemlidir. Bu bilgiyi elde etmek için karmaşıklık matrisine başvurulmalıdır. Şekil 5.1’de hiyerarşik ESA-UKSB modeline ait karmaşıklık matrisi, Şekil 5.2’de paralel ESA-UKSB modeline ait karmaşıklık matrisine yer verilmektedir.



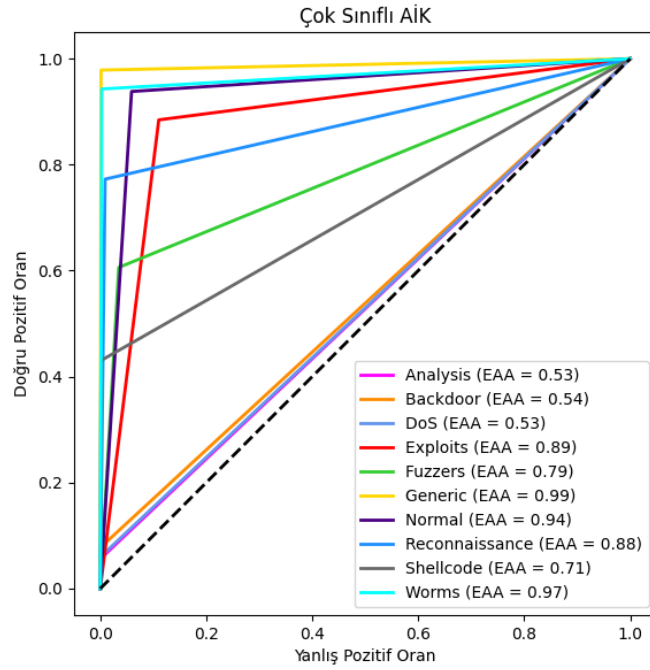
Şekil 5.1. Hiyerarşik ESA-UKSB Modele Ait Karmaşıklık Matrisi (UNSW-NB15)



Şekil 5.2. Paralel ESA-UKSB Modele Ait Karmaşıklık Matrisi (UNSW-NB15)

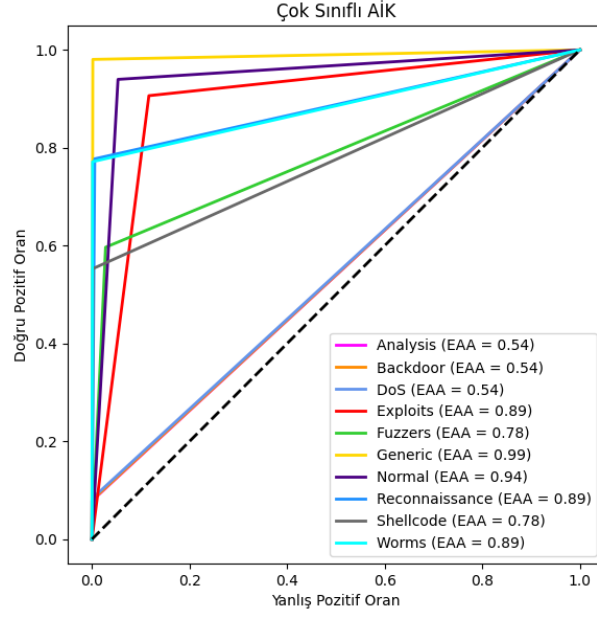
Bu değerler incelendiğinde, iki modelde de "Fuzzer" sınıfına ait verilerin "Normal" sınıf olarak algılandığı gözlemlenmiştir. Ayrıca, dikkat çeken bir diğer husus, "DoS" sınıfının "Exploits" sınıfı ile karışmış olmasıdır.

Çok sınıflı sınıflandırma problemlerinde kullanılan modelde sınıfların gösterdiği doğruluk oranını belirlemek için AİK-EAA eğrisine başvurulmaktadır. Bu çalışmada, UNSW-NB15 veri seti üzerinde hiyerarşik ESA-UKSB modelde elde edilen AİK-EAA eğrisine Şekil 5.3'te yer verilirken, paralel modelde elde edilen AİK-EAA eğrisine Şekil 5.4'te yer verilmektedir.



Şekil 5.3. Hiyerarşik ESA-UKSB Modeline Ait AİK-EAA Eğrisi (UNSW-NB15)

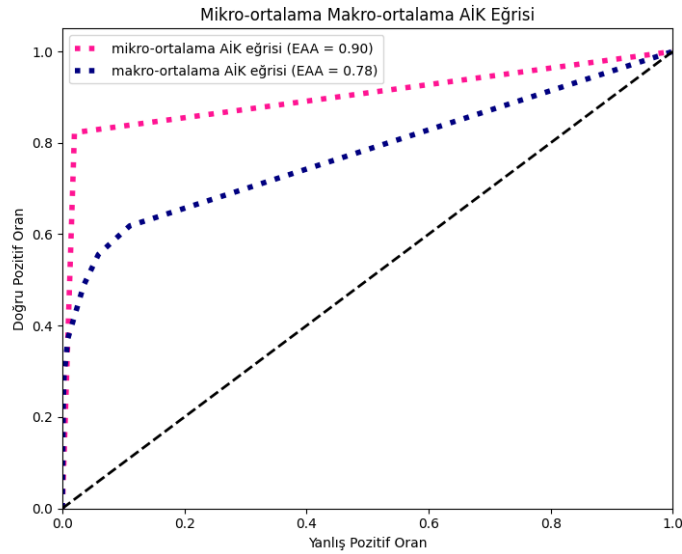
UNSW-NB15 veri seti üzerinden hiyerarşik ESA-UKSB modeline ait AİK-EAA eğrisi incelendiğinde, en düşük sonuç veren sınıfın "Analysis" sınıfı olduğu görülmektedir. Bu sınıf, modelin doğruluk oranını olumsuz etkilemiştir. "Backdoor" ve "DoS" sınıfları da doğruluk oranını düşüren diğer sınıflar arasında yer almaktadır. Öte yandan, en iyi sonuçlar "Generic", "Worms" ve "Normal" sınıflarında elde edilmiştir.



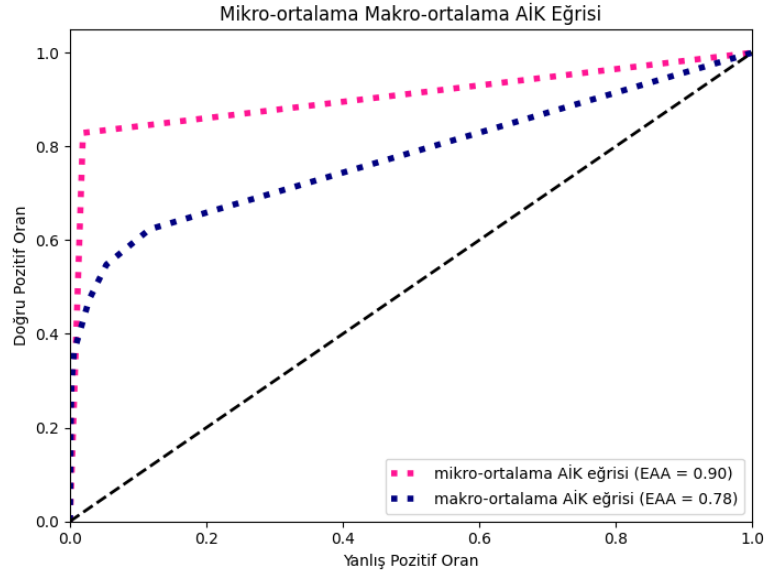
Şekil 5.4. Paralel ESA-UKSB Modeline Ait AİK-EAA Eğrisi (UNSW-NB15)

UNSW-NB15 veri seti üzerinden paralel ESA-UKSB modeline ait AİK-EAA eğrisi incelendiğinde, en düşük sonuç veren sınıfların 0.54 EAA değerine sahip "Backdoor", "Analysis" ve "DoS" olduğu görülmektedir. Bu modelde de en iyi sonuçlar "Generic" ve "Normal" sınıflarında elde edilmiştir.

Son olarak, çok sınıflı sınıflandırma problemlerinde model başarısını ölçmek için başvuru olan diğer iki önemli metrik olan Makro AİK ve Mikro AİK değerlerine ait grafiğe yer verilmektedir. Şekil 5.5'te hiyerarşik ESA-UKSB modeline ait Makro-Mikro AİK eğrilerine yer verilirken Şekil 5.6'da paralel ESA-UKSB modeline ait eğrilere yer verilmiştir.



Şekil 5.5. Hiyerarşik ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (UNSW-NB15)



Şekil 5.6. Paralel ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (UNSW-NB15)

Bu eğriler incelendiğinde UNSW-NB15 veri seti kullanılarak eğitilen her iki model için de aynı sonuçlar üretildiği gözlemlenmiştir. Makro AİK 0.90 EAA değerine sahipken, Mikro AİK 0.78 EAA değerine sahip olduğu görülmektedir.

5.2. AWID Veri Seti Kullanılarak Hiyerarşik ve Paralel ESA-UKSB Modelinin Değerlendirilmesi

Bu başlıkta, paralel ESA-UKSB ve hiyerarşik ESA-UKSB modellerinin AWID veri kümesi üzerinde elde edilen sonuçlarına odaklanılmıştır. UNSW-NB15 veri seti üzerinde yapılan tüm değerlendirmeler, AWID veri seti üzerinde de tekrarlanmıştır. İlk olarak, her iki modelin kullanılmasıyla elde edilen doğruluk skorlarına bakılmıştır. Daha sonra, diğer değerlendirmeler üzerinde durulmuştur. Hiyerarşik ESA-UKSB modelinde elde edilen doğruluk skoru %83,29 iken paralel ESA-UKSB modelinde elde edilen doğruluk skorunun %98,30 olduğu görülmüştür. AWID veri seti üzerinde paralel ESA-UKSB modelinden çok daha iyi sonuçlar elde edilmiştir. Sonuçları daha iyi incelemek için diğer değerlere aşağıda yer verilmiştir.

AWID veri kümesi üzerinde her bir sınıf için hesaplanan F1 Skor, hassasiyet ve duyarlılık metrikleri değerleri hiyerarşik ESA-UKSB model için Tablo 5.3'te paralel ESA-UKSB model için Tablo 5.4'te sunulmaktadır.

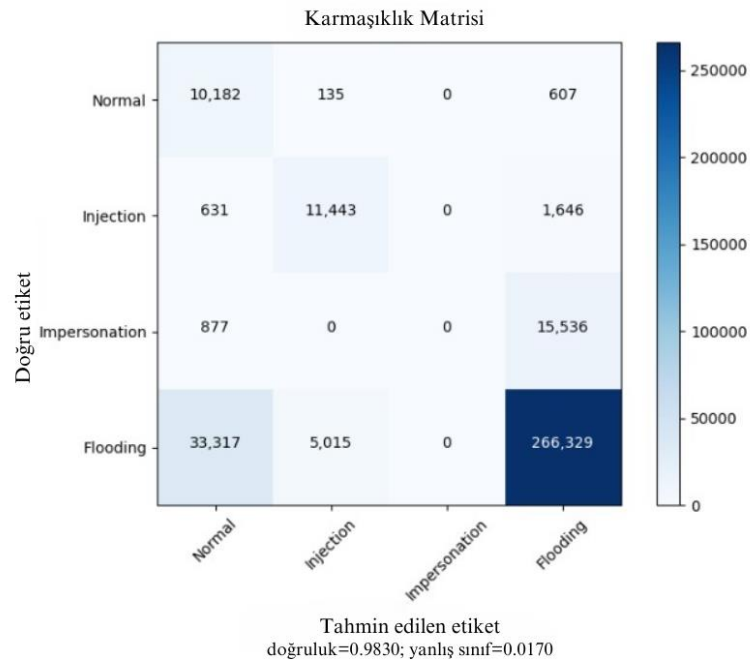
Tablo 5.3. Hiyerarşik ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (AWID)

Sınıf	Hassasiyet (Hiyerarşik ESA-UKSB)	Duyarlılık (Hiyerarşik ESA-UKSB)	F1 Skor (Hiyerarşik ESA-UKSB)
Normal	0.23	0.93	0.36
Injection	0.69	0.83	0.75
Impersonation	0.00	0.00	0.00
Flooding	0.94	0.87	0.90

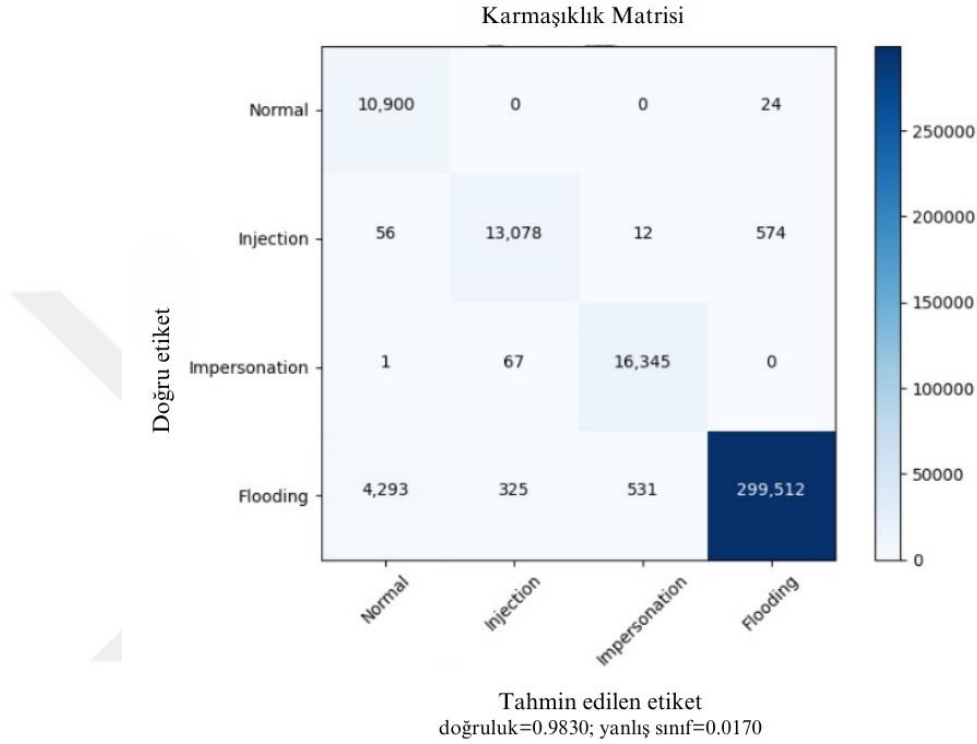
Tablo 5.4. Paralel ESA-UKSB Modeline Ait Sınıfların Metrik Değerleri (AWID)

Sınıf	Hassasiyet (Hiyerarşik ESA-UKSB)	Duyarlılık (Hiyerarşik ESA-UKSB)	F1 Skor (Hiyerarşik ESA-UKSB)
Normal	0.71	1.00	0.83
Injection	0.97	0.95	0.96
Impersonation	0.97	1.00	0.98
Flooding	1.00	0.98	0.99

AWID veri setinde, her iki model için elde edilen karmaşıklık matrislerine bakarak hangi sınıfların karıştığı görülecektir. Şekil 5.7’de hiyerarşik ESA-UKSB modeline ait karmaşıklık matrisi, Şekil 5.8’de ise paralel ESA-UKSB modeline ait karmaşıklık matrisi sunulmaktadır. Bu matrisler, modelin sınıfları ne kadar doğru veya yanlış tahmin ettiğini ayrıntılı bir şekilde göstermektedir.

**Şekil 5.7.** Hiyerarşik ESA-UKSB Modele Ait Karmaşıklık Matrisi (AWID)

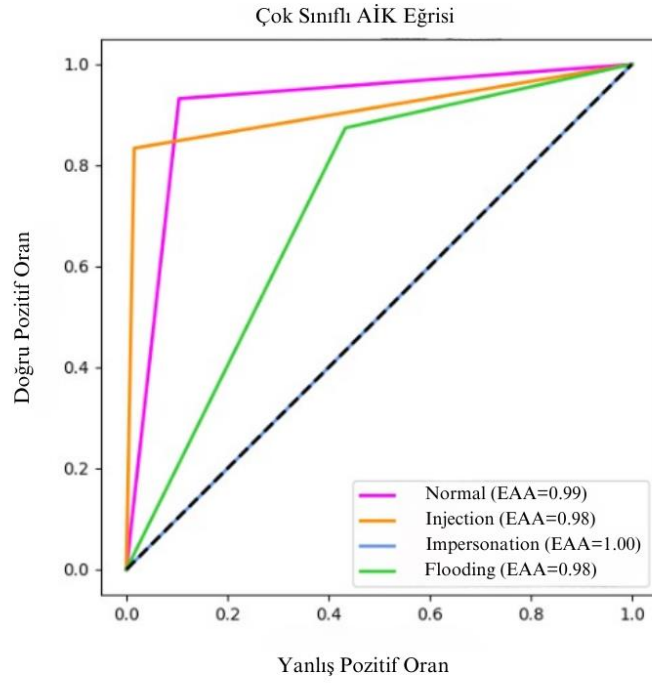
Hiyerarşik ESA-UKSB modelinde “Impersonation” sınıfında tahmin edilen etiketin gerçek etikete eşit olduğu değer 0 olarak hesaplanmıştır. Bu sınıf “Normal” ve “Flooding” sınıfı ile karıştığı için modelin doğruluk oranını aşağıya çekmiştir.



Şekil 5.8. Paralel ESA-UKSB Modele Ait Karmaşıklık Matrisi (AWID)

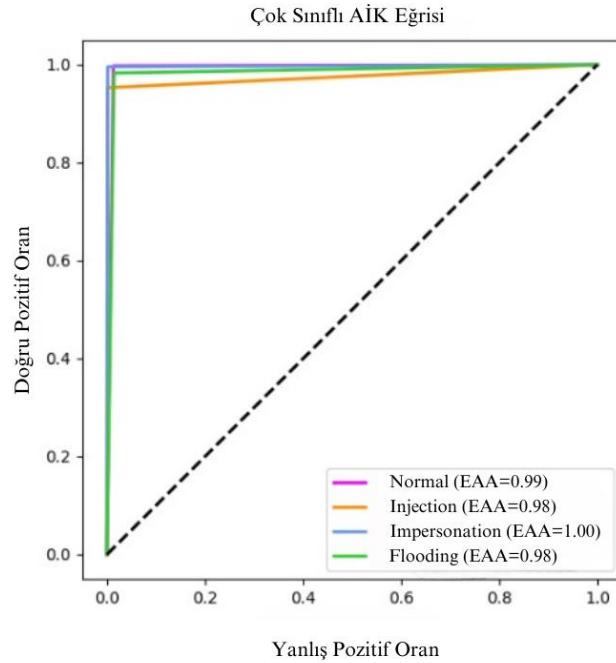
Paralel ESA-UKSB modeline bakıldığında, “Impersonation” sınıfı hiyerarşik ESA-UKSB modeline göre daha iyi performans göstermiş bu da doğruluk oranını doğrudan yükseltmiştir.

Yukarıda çok sınıflı sınıflandırma problemlerinde sınıfların gösterdiği doğruluk oranını daha iyi görebilmek için AİK-EAA eğrisinden faydalandığından bahsedilmiştir. Oluşturulan modelleri sınıfsal olarak değerlendirebilmek için AWID veri seti üzerinde elde edilen AİK-EAA eğrileri sunulmuştur. Hiyerarşik ESA-UKSB modelde elde edilen AİK-EAA eğrisi Şekil 5.9’da yer verilirken, paralel modelde elde edilen AİK-EAA eğrisine Şekil 5.10’da yer verilmektedir.



Şekil 5.9. Hiyerarşik ESA-UKSB Modeline Ait AİK-EAA Eğrisi (AWID)

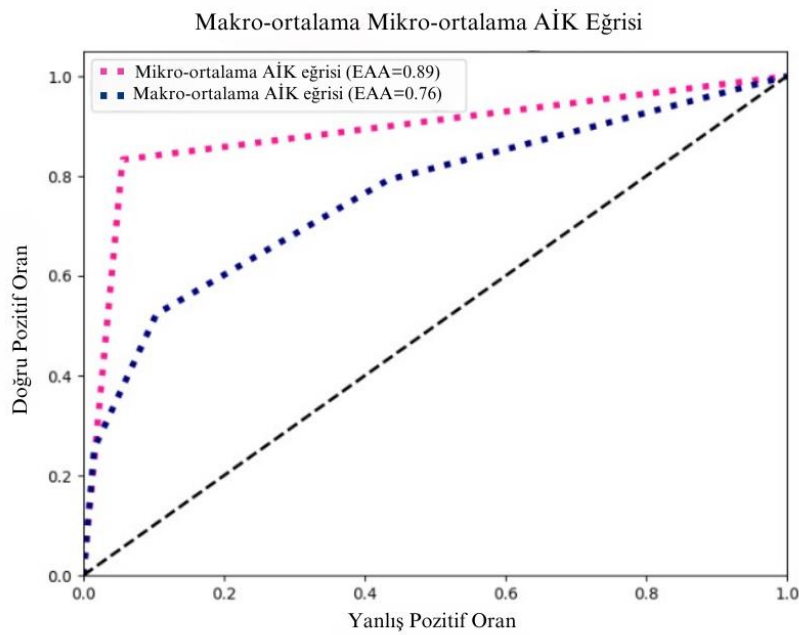
EAA değerinin 0.50 olması “Impersonation” sınıfının rastgele tahmin yapmasına benzer bir performans sergilediğini göstermektedir. AWID üzerinde hiyerarşik ESA-UKSB modelinde “Impersonation” sınıfında doğru değerler üretilmemiştir. Bunun yanında “Normal” ve “Injection” sınıfları 0.91 EAA değerine sahip olup yüksek performans sergilemektedir.



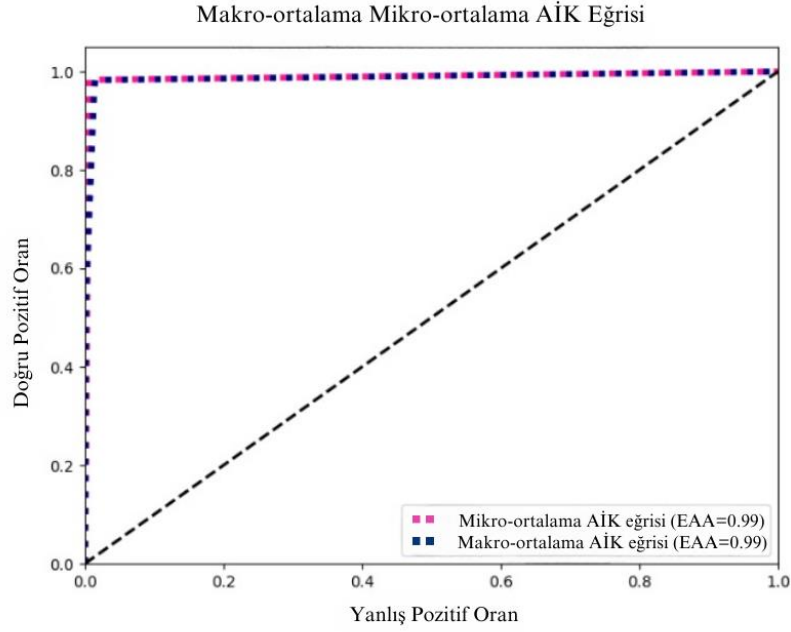
Şekil 5.10. Paralel ESA-UKSB Modeline Ait AİK-EAA Eğrisi (UNSW-NB15)

Hiyerarşik ESA-UKSB modelin aksine paralel ESA-UKSB modelde en iyi performansı “Impersonation” sınıfı göstermektedir. Diğer sınıfların da EAA değerleri 1 değerine yakın olduğu için mükemmel performans göstermektedirler.

AWID veri seti üzerinde son olarak Makro AİK ve Mikro AİK eğrilerine yer verilecektir. Şekil 5.11’de hiyerarşik ESA-UKSB modeline, Şekil 5.12’de paralel ESA-UKSB modeline ait Makro AİK, Mikro AİK eğrileri bulunmaktadır.



Şekil 5.11. Hiyerarşik ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (AWID)



Şekil 5.12. Paralel ESA-UKSB Modeline Makro-Mikro AİK Eğrisi (AWID)

AWID veri seti üzerinde paralel ESA-UKSB modelinin, hiyerarşik ESA-UKSB modele göre daha iyi bir performans gösterdiği hem Makro AİK hem de Mikro AİK eğrilerinde gözlemlenmektedir. Paralel ESA-UKSB modeline ait Makro AİK ve Mikro AİK EAA değerleri 0.99 olarak hesaplanmıştır. Diğer yandan, hiyerarşik ESA-UKSB modele ait Makro AİK EAA değeri 0.76 iken Mikro AİK EAA değeri 0.89 olarak belirlenmiştir. Bu bulgular, paralel modelin daha üstün bir performans sergilediğini ortaya koymaktadır.

6. SONUÇLAR VE TARTIŞMA

Bu çalışmada, bulut altyapısında meydana gelebilecek saldırıları tespit etmek için derin öğrenme yöntemleri kullanılarak iki sınıflandırma modeli önerilmektedir. Bu modeller iki derin öğrenme algoritmasının birleştirilmesiyle elde edilmiştir. Oluşturulan modelleri test etmek amacıyla saldırı ve normal ağ trafiğinin izlendiği iki farklı veri seti kullanılmaktadır. Beşinci bölümde verilen sonuçlara dayanarak, çalışma ile ilgili çıkarımlar ve genel değerlendirmeler aşağıda sunulmuştur:

- Bu çalışmada elde edilen sonuçlar derin öğrenme yöntemlerini ağ saldırı tespitinde başarılı sonuçlar üretebileceği görülmüştür.
- AWID veri seti üzerinde paralel ESA-UKSB modelinin doğruluk skoru %98,30 olarak hiyerarşik ESA-UKSB modelinin doğruluk skoru %83,29 olarak saptanmıştır. Bu da paralel modelin daha yüksek performans sergilediğini göstermektedir.
- UNSW-NB15 veri seti üzerinde paralel ESA-UKSB modelinin doğruluk skoru %82,89 olarak hiyerarşik ESA-UKSB modelinin doğruluk skoru %82,24 olduğu görülmektedir. Bu veri seti üzerinde her iki modelin doğruluk oranlarının orantılı olduğu görülmüştür.
- UNSW-NB15 veri seti üzerinde kullanılan her iki modelde de "Fuzzers" sınıfına ait verilerin "Normal" sınıfı ile, "DoS" sınıfına ait verilerin ise "Exploits" sınıfı ile karışmış olması dikkat çekmektedir.
- UNSW-NB15 veri seti üzerinden yapılan inceleme, hiyerarşik ESA-UKSB modeline ait sonuçların en düşük olduğu sınıfın "Analysis" sınıfı olduğunu göstermektedir. Ayrıca, "Backdoor" ve "DoS" sınıfları da doğruluk oranını düşüren diğer sınıflar arasında bulunmaktadır. Bununla birlikte, en yüksek doğruluk sonuçları "Generic", "Worms" ve "Normal" sınıflarında elde edilmiştir.
- UNSW-NB15 veri seti üzerinde paralel ESA-UKSB modeline ait sonuçlar incelendiğinde, en düşük sonuçlar "Backdoor" ve "DoS" sınıflarında elde edilmiştir. Diğer olumsuz bir sonuç veren sınıf ise "Analysis" sınıfıdır. Bu modelde de hiyerarşik ESA-UKSB modelinde olduğu gibi en iyi sonuçlar "Generic", "Worms" ve "Normal" sınıflarında elde edilmiştir.
- AWID veri seti üzerinden hiyerarşik ESA-UKSB modelinde "Impersonation" sınıfında tahmin edilen etiketin gerçek etikete eşit olduğu değer 0 olarak hesaplanmıştır. Sonuçlar incelendiğinde bu sınıf "Normal" ve "Flooding" sınıfları ile karıştığı görülmektedir.
- AWID veri seti üzerinden hiyerarşik ESA-UKSB modelin aksine paralel ESA-UKSB modeli "Impersonation" sınıfı üzerinde daha iyi sonuçlar elde edildiği görülmektedir.

- Güvenlik tehditlerinin karmaşıklığı ve hacmi arttıkça, derin öğrenme algoritmaları, bulut sistemlerindeki güvenlik açıklarını tespit etme, saldırıları önleme ve veri gizliliğini sağlama konularında etkin bir rol oynayabilirler.

Genel olarak çalışma incelendiğinde, derin öğrenme algoritmaları olan ESA ve UKSB algoritmalarının birleştirilmesiyle, verilerin hem mekânsal hem de zamansal özelliklerini öğrenebilen hibrit bir yapı oluşturulmuştur. Değerlendirmeler sonucunda her yaklaşımın kendine özgü avantajları ve dezavantajları olduğu tespit edilmiştir. Genel olarak, ESA ve UKSB kullanılarak oluşturulan kombinasyonunun kullanılması, saldırı tespitinin başarıyla üstesinden gelmek için güçlü bir araç sunabilir.



ÖNERİLER

Bu tez çalışması, bulut bilişim teknolojisinin önümüzdeki yıllarda daha fazla yaygınlaşacağına dair bir gözlemi temel alıyor. Bu yaygınlaşma, işletmelerin ve bireylerin verilerini ve hizmetlerini buluta taşımasını hızlandırmaktadır. Ancak, bu durum bulut güvenliği konusunda daha fazla sorumluluk ve dikkat gerektiriyor. Çünkü verilerin ve hizmetlerin bulutta saklanması, güvenlik açısından yeni zorluklar ve riskler ortaya çıkarıyor. Bu nedenle, bulut bilişimin her katmanının güvenliğine odaklanmak kritik bir öneme sahiptir.

Bu çalışmada, bulut güvenliği alanında ortaya çıkan ağ saldırılarına karşı çözümler sunmak amacıyla hibrit derin öğrenme modelleri geliştirilmiştir. Derin öğrenme modelleri, büyük veri setleri üzerinde eğitildiğinde yüksek başarı elde edebilir. Ancak, model seçimi süreci dikkatlice yapılmalıdır. Veri setinin özellikleri ve gereksinimleri, hangi derin öğrenme modelinin kullanılacağını belirlemede kritik bir rol oynar. Ayrıca, hiperparametre ayarlaması ve çapraz doğrulama gibi optimizasyon teknikleri kullanarak modelin performansını en üst düzeye çıkarmak önemlidir. Bu teknikler, modelin eğitim sürecinin daha etkili olmasına yardımcı olabilir, aşırı öğrenmeyi önleyebilir ve genelleme yeteneğini artırabilir.

Derin öğrenmenin siber güvenlik alanında kullanılması daha güçlü ve etkili çözümler sunabilir. Derin öğrenme modelleri, büyük veri miktarlarını işleme ve karmaşık desenleri tanımlama yetenekleri sayesinde, güvenlik açısından kritik olan alanlarda önemli bir rol oynayabilirler. Ancak, bu modeller güvenli bir şekilde kullanılmalı ve eğitilmelidir, aksi takdirde daha kötü sonuçlarla karşılaşılabilir.

KAYNAKLAR

- [1] Mell, P. ve Grance, T. (2011). The NIST definition of cloud computing.
- [2] Tulloch, M. (2013). *Introducing Windows Azure for IT Professionals*. Microsoft Press.
- [3] Madhavaiah, C. ve Bashir, I. (2012). Defining cloud computing in business perspective: A review of research. *Metamorphosis*, 11(2), 50-65.
- [4] Kulkarni, G., Sutar, R. ve Gambhir, J. (2012). Cloud computing-Infrastructure as service-Amazon EC2. *International journal of Engineering research and applications*, 2(1), 117-125.
- [5] Kuyoro, S. O., Ibikunle, F. ve Awodele, O. (2011). Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, 3(5), 247-255.
- [6] Sheik, S. A. ve Muniyandi, A. P. (2023). Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. *Cyber Security and Applications*, 1, 100002.2.
- [7] Jadeja, Y. ve Modi, K. (2012). Cloud computing-concepts, architecture and challenges. In 2012 international conference on computing, electronics and electrical technologies (ICCEET) (pp. 877-880). IEEE.
- [8] Kebande, V. R. ve Venter, H. S. (2014). A cognitive approach for botnet detection using Artificial Immune System in the cloud. In 2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 52-57). IEEE.
- [9] Osanaiye, O., Cai, H., Choo, K. K. R., Dehghantanha, A., Xu, Z. ve Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking*, 2016(1), 1-10.
- [10] Zhang, F., Huang, Y., Wang, H., Chen, H. ve Zang, B. (2008). PALM: security preserving VM live migration for systems with VMM-enforced protection. In 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference (pp. 9-18). IEEE.
- [11] Neelakantan, P. (2023). A secure framework for the cloud to protect the virtual machine from malicious events. *Multimedia Tools and Applications*, 1-24.
- [12] Jelidi, M., Ghourabi, A. ve Gasmi, K. (2019). A hybrid intrusion detection system for cloud computing environments. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
- [13] Mishra, P., Pilli, E. S., Varadharajant, V. ve Tupakula, U. (2016). NvCloudIDS: A security architecture to detect intrusions at network and virtualization layer in cloud environment. In 2016 international conference on advances in computing, communications and informatics (ICACCI) (pp. 56-62). IEEE.
- [14] El-Kassabi, H. T., Serhani, M. A., Masud, M. M., Shuaib, K. ve Khalil, K. (2023). Deep learning approach to security enforcement in cloud workflow orchestration. *Journal of Cloud Computing*, 12(1), 1-22.

- [15] Kumar, A., Umurzoqovich, R. S., Duong, N. D., Kanani, P., Kuppusamy, A., Praneesh, M. ve Hieu, M. N. (2022). An intrusion identification and prevention for cloud computing: From the perspective of deep learning. *Optik*, 270, 170044.
- [16] Pandey, B. K., Veeramanickam, M. R. M., Ahmad, S., Rodriguez, C. ve Esenarro, D. (2023). ExpSSOA-Deep maxout: Exponential Shuffled shepherd optimization based Deep maxout network for intrusion detection using big data in cloud computing framework. *Computers & Security*, 124, 102975.
- [17] Akgun, D., Hizal, S. ve Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security*, 118, 102748.
- [18] Lin, H., Xue, Q., Feng, J. ve Bai, D. (2023). Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine. *Digital Communications and Networks*, 9(1), 111-124.
- [19] Wu, P. ve Guo, H. (2019). LuNET: a deep neural network for network intrusion detection. In *2019 IEEE symposium series on computational intelligence (SSCI)* (pp. 617-624). IEEE.
- [20] McCarthy, J. (1992). Reminiscences on the history of time-sharing. *IEEE Annals of the History of Computing*, 14(1), 19-24.
- [21] Hauben, M. (2007). History of ARPANET. Site de l'Instituto Superior de Engenharia do Porto, 17, 1-20.
- [22] Opitz, N., Langkau, T. F., Schmidt, N. H. ve Kolbe, L. M. (2012, January). Technology acceptance of cloud computing: empirical evidence from German IT departments. In *2012 45th Hawaii International Conference on System Sciences* (pp. 1593-1602). IEEE.
- [23] Mathew, S. ve Varia, J. (2014). Overview of amazon web services. *Amazon Whitepapers*, 105, 1-22.
- [24] Dillon, T., Wu, C. ve Chang, E. (2010). Cloud computing: issues and challenges. In *2010 24th IEEE international conference on advanced information networking and applications* (pp. 27-33). Ieee.
- [25] Diaby, T. ve Rad, B. B. (2017). Cloud computing: a review of the concepts and deployment models. *International Journal of Information Technology and Computer Science*, 9(6), 50-58.
- [26] Kuyoro, S. O., Ibikunle, F. ve Awodele, O. (2011). Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, 3(5), 247-255.
- [27] Goyal, S. (2014). Public vs private vs hybrid vs community-cloud computing: a critical review. *International Journal of Computer Network and Information Security*, 6(3), 20-29.
- [28] Gibson, J., Rondeau, R., Eveleigh, D. ve Tan, Q. (2012). Benefits and challenges of three cloud computing service models. In *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)* (pp. 198-205). IEEE.
- [29] Rashid, A. ve Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. *International Journal of Computer Sciences and Engineering*, 7(2), 421-426.

- [30] Ashraf, I. (2014). An overview of service models of cloud computing. *International Journal of Multidisciplinary and Current Research*, 2(1), 779-783.
- [31] Satyanarayana, S. (2012). Cloud computing: SAAS. *Computer Sciences and Telecommunications*, (4), 76-79.
- [32] Thomas, D. (2008). Enabling application agility: software as a service, cloud computing and dynamic languages. *Journal of object technology*, 7(4), 29-32.
- [33] Zissis, D. ve Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, 28(3), 583-592.
- [34] Kumar, P. R., Raj, P. H. ve Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, 125, 691-697.
- [35] Vaquero, L. M., Rodero-Merino, L. ve Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. *Computing*, 91, 93-118.
- [36] Tabrizchi, H. ve Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, 76(12), 9493-9532.
- [37] Suryateja, P. S. (2018). Threats and vulnerabilities of cloud computing: a review. *International Journal of Computer Sciences and Engineering*, 6(3), 297-302.
- [38] Isharufe, W., Jaafar, F. ve Butakov, S. (2020). Study of security issues in platform-as-a-service (paas) cloud model. In *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)* (pp. 1-6). IEEE.
- [39] Sandikkaya, M. T. ve Harmanci, A. E. (2012). Security problems of platform-as-a-service (paas) clouds and practical solutions to the problems. In *2012 IEEE 31st Symposium on Reliable Distributed Systems* (pp. 463-468). IEEE.
- [40] Hashizume, K., Rosado, D. G., Fernández-Medina, E. ve Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, 4, 1-13.
- [41] Anjana ve Singh, A. (2019). Security concerns and countermeasures in cloud computing: a qualitative analysis. *International Journal of Information Technology*, 11, 683-690.
- [42] Rath, A., Spasic, B., Boucart, N. ve Thiran, P. (2019). Security pattern for cloud SaaS: From system and data security to privacy case study in AWS and Azure. *Computers*, 8(2), 34.
- [43] Wen, P. X. ve Dong, L. (2013). Quality model for evaluating SaaS service. In *2013 Fourth international conference on emerging intelligent data and web technologies* (pp. 83-87). IEEE.
- [44] Fortino, G., Parisi, D., Pirrone, V. ve Di Fatta, G. (2014). BodyCloud: A SaaS approach for community body sensor networks. *Future Generation Computer Systems*, 35, 62-79.
- [45] Kanade, S. ve Manza, R. (2019). A Comprehensive Study on Multi Tenancy in SAAS Applications. *International Journal of Computer Applications*, 181(44), 25-27.
- [46] Almorsy, M., Grundy, J. ve Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

- [47] Bisong, A. ve Rahman, M. (2011). An overview of the security concerns in enterprise cloud computing. arXiv preprint arXiv:1101.5613.
- [48] Arora, R., Parashar, A. ve Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. *International journal of engineering research and applications*, 3(4), 1922-1926.
- [49] Younis, Y. A., Kifayat, K. ve Merabti, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications*, 19(1), 45-60.
- [50] Choudhury, A. J., Kumar, P., Sain, M., Lim, H. ve Jae-Lee, H. (2011). A strong user authentication framework for cloud computing. In *2011 IEEE Asia-Pacific Services Computing Conference* (pp. 110-115). IEEE.
- [51] Kazim, M. ve Zhu, S. Y. (2015). A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications*, 6(3), 109-113.
- [52] Banyal, R. K., Jain, P. ve Jain, V. K. (2013). Multi-factor authentication framework for cloud computing. In *2013 fifth international conference on computational intelligence, modelling and simulation* (pp. 105-110). IEEE.
- [53] Low, C., Chen, Y. ve Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial management & data systems*.
- [54] Weir, G. R. ve Aßmuth, A. (2017). Strategies for intrusion monitoring in cloud services. In *The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization* (pp. 1-5).
- [55] Grobauer, B., Walloschek, T. ve Stocker, E. (2010). Understanding cloud computing vulnerabilities. *IEEE Security & privacy*, 9(2), 50-57.
- [56] Shim, J. ve Lim, Y. (2013). Implementation of real time alert system over cloud computing. *International Journal of Energy, Information & Communications*, 4(3).
- [57] Zhang, X., Wuwong, N., Li, H. ve Zhang, X. (2010). Information security risk management framework for the cloud computing environments. In *2010 10th IEEE international conference on computer and information technology* (pp. 1328-1334). IEEE.
- [58] Ramgovind, S., Eloff, M. M. ve Smith, E. (2010). The management of security in cloud computing. In *2010 Information Security for South Africa* (pp. 1-7). IEEE.
- [59] Zarrabi, A. ve Zarrabi, A. (2012). Internet intrusion detection system service in a cloud. *International Journal of Computer Science Issues (IJCSI)*, 9(5), 308.
- [60] Bazm, M. M., Lacoste, M., Südholt, M. ve Menaud, J. M. (2019). Isolation in cloud computing infrastructures: new security challenges. *Annals of Telecommunications*, 74, 197-209.
- [61] Wu, H., Ding, Y., Winer, C. ve Yao, L. (2010). Network security for virtual machine in cloud computing. In *5th International conference on computer sciences and convergence information technology* (pp. 18-21). IEEE.

- [62] Factor, M., Hadas, D., Harnama, A., Har'El, N., Kolodner, E. K., Kurmus, A. ve Sorniotti, A. (2013). Secure logical isolation for multi-tenancy in cloud storage. In *2013 IEEE 29th Symposium on Mass Storage Systems and Technologies (MSST)* (pp. 1-5). IEEE.
- [63] LeCun, Y., Bengio, Y. ve Hinton, G. (2015). Deep learning. *nature*, 521(7553), 436-444.
- [64] Thapa, N., Liu, Z., Kc, D. B., Gokaraju, B. ve Roy, K. (2020). Comparison of machine learning and deep learning models for network intrusion detection systems. *Future Internet*, 12(10), 167.
- [65] Bhatt, C., Kumar, I., Vijayakumar, V., Singh, K. U. ve Kumar, A. (2021). The state of the art of deep learning models in medical science and their challenges. *Multimedia Systems*, 27(4), 599-613.
- [66] Nielsen, M. A. (2015). *Neural networks and deep learning* (Vol. 25, pp. 15-24). San Francisco, CA, USA: Determination press.
- [67] Albawi, S., Mohammed, T. A. ve Al-Zawi, S. (2017). Understanding of a convolutional neural network. In *2017 international conference on engineering and technology (ICET)* (pp. 1-6). Ieee.
- [68] Li, Z., Liu, F., Yang, W., Peng, S. ve Zhou, J. (2021). A survey of convolutional neural networks: analysis, applications, and prospects. *IEEE transactions on neural networks and learning systems*.
- [69] Medsker, L. R. ve Jain, L. C. (2001). Recurrent neural networks. *Design and Applications*, 5, 64-67.
- [70] Sherstinsky, A. (2020). Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. *Physica D: Nonlinear Phenomena*, 404, 132306.
- [71] Vinayakumar, R., Soman, K. P., Poornachandran, P. ve Sachin Kumar, S. (2018). Detecting Android malware using long short-term memory (LSTM). *Journal of Intelligent & Fuzzy Systems*, 34(3), 1277-1288.
- [72] <https://ishakdolek.medium.com/lstm-d2c281b92aac>, Eriřim: 12 řubat 2018
- [73] Chalapathy, R. ve Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*.
- [74] Munir, M., Siddiqui, S. A., Dengel, A. ve Ahmed, S. (2018). DeepAnT: A deep learning approach for unsupervised anomaly detection in time series. *Ieee Access*, 7, 1991-2005.
- [75] Malaiya, R. K., Kwon, D., Suh, S. C., Kim, H., Kim, I. ve Kim, J. (2019). An empirical evaluation of deep learning for network anomaly detection. *IEEE Access*, 7, 140806-140817.
- [76] Sohi, S. M., Seifert, J. P. ve Ganji, F. (2021). RNNIDS: Enhancing network intrusion detection systems through deep learning. *Computers & Security*, 102, 102151.
- [77] Applebaum, S., Gaber, T. ve Ahmed, A. (2021). Signature-based and machine-learning-based web application firewalls: A short survey. *Procedia Computer Science*, 189, 359-367.
- [78] Nivaashini, M. ve Thangaraj, P. (2018). A framework of novel feature set extraction based intrusion detection system for internet of things using hybrid machine learning algorithms. In *2018 International conference on computing, power and communication technologies (GUCON)* (pp. 44-49). IEEE.

- [79] Li, Y., Qin, T., Huang, Y., Lan, J., Liang, Z. ve Geng, T. (2022). HDFEF: A hierarchical and dynamic feature extraction framework for intrusion detection systems. *Computers & Security*, 121, 102842.
- [80] Callegari, C., Bucchianeri, E., Giordano, S. ve Pagano, M. (2019). Real time attack detection with deep learning. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 1-5). IEEE.
- [81] Aminanto, M. E. ve Kim, K. (2017). Detecting impersonation attack in WiFi networks using deep learning approach. In *Information Security Applications: 17th International Workshop, WISA 2016, Jeju Island, Korea, August 25-27, 2016, Revised Selected Papers 17* (pp. 136-147). Springer International Publishing.
- [82] <https://insideaiml.com/blog/SoftMaxActivation-Function-1034>, Erişim: Mayıs 2023
- [83] Zhu, D., Lu, S., Wang, M., Lin, J. ve Wang, Z. (2020). Efficient precision-adjustable architecture for softmax function in deep learning. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67(12), 3382-3386.
- [84] Berrar, D. (2019). Cross-Validation.
- [85] Szeghalmy, S., & Fazekas, A. (2023). A Comparative Study of the Use of Stratified Cross-Validation and Distribution-Balanced Stratified Cross-Validation in Imbalanced Learning. *Sensors*, 23(4), 2333.
- [86] <https://medium.com/@mijanr/different-ways-to-combine-cnn-and-lstm-networks-for-time-series-classification-tasks-b03fc37e91b6> Erişim: 26 Ağustos 2021
- [87] Yacoub, R. ve Axman, D. (2020). Probabilistic extension of precision, recall, and f1 score for more thorough evaluation of classification models. In *Proceedings of the first workshop on evaluation and comparison of NLP systems* (pp. 79-91).
- [88] Flach, P. ve Kull, M. (2015). Precision-recall-gain curves: PR analysis done right. *Advances in neural information processing systems*, 28.
- [89] Krstinić, D., Braović, M., Šerić, L., & Božić-Štulić, D. (2020). Multi-label classifier performance evaluation with confusion matrix. *Computer Science & Information Technology*, 1.
- [90] Marzban, C. (2004). The ROC curve and the area under it as performance measures. *Weather and Forecasting*, 19(6), 1106-1114.
- [91] Scikit-learn, https://scikit-learn.org/stable/auto_examples/model_selection/plot_roc.html Erişim: 1 Şubat 2010

ÖZGEÇMİŞ

Tuğba TEKKOL

[illegible]

■ [REDACTED]

■ [REDACTED]

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

[REDACTED]
[REDACTED] in [REDACTED]
[REDACTED]