



**T.C.
BATMAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

AKILLI SALDIRI TESPİT SİSTEMLERİ

Hanifi TOPRAK

YÜKSEK LİSANS TEZİ

Elektrik Elektronik Mühendisliği Anabilim Dalı

**Şubat-2021
BATMAN
Her Hakkı Saklıdır**

TEZ KABUL VE ONAYI

Hanifi TOPRAK tarafından hazırlanan **AKILLI SALDIRI TESPİT SİSTEMLERİ** adlı tez çalışması 17/02/2021 tarihinde aşağıdaki jüri tarafından oy birliği ile Batman Üniversitesi Fen Bilimleri Enstitüsü Elektrik ve Elektronik Mühendisliği Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri

İmza

Başkan

Doç. Dr. Ömer Faruk ERTUĞRUL

Danışman

Dr. Öğr. Üyesi Süleyman KARDAŞ

Üye

Dr. Öğr. Üyesi Cafer BUDAK

Yukarıdaki sonucu onaylarım.

Prof. Dr. Şahnaz TİĞREK
FBE Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Hanifi TOPRAK

Tarih:

ÖZET
YÜKSEK LİSANS TEZİ
AKILLI SALDIRI TESPİT SİSTEMLERİ

Hanifi TOPRAK

Batman Üniversitesi Fen Bilimleri Enstitüsü
Elektrik Elektronik Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Süleyman KARDAŞ

2021, 88 Sayfa

Jüri

Danışman Dr. Öğr. Üyesi Süleyman KARDAŞ
Doç. Dr. Ömer Faruk ERTUĞRUL
Dr. Öğr. Üyesi Cafer BUDAK

Bilgi ve İletişim Teknolojileri hayatımızın her alanını içine alan insanların hatta tüm canlıların ayrılmaz bir parçası haline gelmiştir. Bunun hayatımıza artarak dokunması beklenmektedir. Teknolojinin bu kadar hayatımızla iç içe geçmesi nedeni ile bunu kendi amaçları doğrultusunda kullanmak isteyenlerin ortaya çıkması da beklenendir. Teknolojinin birçok faydası bulunmaktadır. Fakat güvenlik açısından gerekli hassasiyet gösterilmemesi durumunda ise istenilmeyen sonuçlar da doğabilmektedir. Saldırganlar özellikle toplumu en çok etkileyen alanlardan olan Bankacılık, Enerji, Ulaşım gibi sistemlere sızmaya ya da kullanılmaz hale getirmeye çalışırlar. Saldırgan için motivasyon kaynağı bazen para, bazen de şan-şöhret olabilmektedir. Teknolojinin olduğu her yerde bir güvenlik problemi olduğu herkesin kabul ettiği bir gerçektir. Bundan dolayı kurumlar kendi siber olaylara müdahale ekiplerini (SOME) oluştururken topyekûn siber savaşlar için ülke çapında USOM kurulmuştur.

Siber saldırı, siber suçluların bir veya daha fazla cihazı tek veya birden fazla cihaza ya da ağa karşı kullanarak başlattığı bir saldırıdır. Siber saldırı ile saldırgan, sistemleri devre dışı bırakabilir, sistemlerden veri çalabilir ya da verilerde değişiklik yapabilir. Siber saldırganlar hedef sistem (ler)e erişmek için türlü teknik ve sosyal mühendislik yollarına başvurur.

Saldırı Tespit Sistemleri (Intrusion Detection Systems), olası saldırıları tespit etmekte kullanılan güvenlik bileşenlerinden biridir. STS, yapılan atakları genel olarak 3 farklı şekilde tespit etmeye çalışır. **İmza Tabanlı STS:** Bu saldırı tespit sisteminde, ağda oluşabilecek bir anormallik mevcut kötü yazılım veri tabanı ile karşılaştırma yapılarak tespit edilir. **Anomali Tabanlı STS:** Bu saldırı tespit sisteminde, kullanıcı profilleri oluşturulmaktadır. Bu profillerin dışına çıkılması durumunda sistem, yapılan işlemi saldırı olarak yorumlanmaktadır. **Protokol Analizi STS:** Protokol aktiviteleri profilleri çıkarılır. Şüpheli bir aktivite ile karşılaşıldığında mevcut profillerle karşılaştırılır. Karşılaştırma sonucunda saldırı olup olmadığına karar verilir.

KDD'99: KDD'99 saldırı tespit sistemleri için model dizayn etmede kullanılan bir veri setidir. Bu veri seti 42 sütun ve 4.940.200 adet satırdan oluşmaktadır. Veri setinde bulunan saldırılar 4 ana kategoride tanımlanabilir: **DoS:** Denial-of-service, ağda bulunan bir sistem ya da cihazın sistem kaynaklarını tüketerek gerçek

kullanıcılara hizmet veremeyecek duruma getirmesidir. Bu saldırı yöntemine syn flood saldırısı örnek olarak verilebilir. **R2L**: Bir sisteme erişim izni olmadan bağlanmaya çalışma saldırılarıdır. Bu saldırı yöntemine guessing password aldırısı örnek olarak verilebilir. **U2R**: Normal kullanıcı yetkisine sahip bir hesabın admin ya da root kullanıcı haklarını elde etme amaçlı yapılan saldırı türüdür. Bu saldırı yöntemine buffer overflow aldırısı örnek olarak verilebilir. **Probing**: Bu saldırıda saldırgan, hedef cihaz hakkında bilgi toplamaktadır. Bu bilgi; açık olan portlar, geçerli ip adresleri, üzerinde çalışan servisler, kurulu olan işletim sistemi olabilmektedir. Port scanning probing saldırılarına örnek verilebilir.

Bu tezde, saldırı tespit sistemlerinde kullanılan KDD'99 veri setinde bulunan saldırılar kategorize edilerek, saldırı istatistikleri ve bu saldırılar hakkında bilgiler verilmiştir. Ayrıca denetimli öğrenme modellerinden olan Yapay Sinir Ağları (YSA) ve Karar Ağaç algoritmaları kullanılarak yapılabilecek bir saldırıyı gerçek zamanlı ve yüksek başarımlı tespit edecek sistem modelleri yapılmıştır.

Anahtar Kelimeler: Akıllı Saldırı Tespit Sistemleri, KDD'99, Siber Güvenlik, Karar Ağaçları, Yapay Sinir Ağları, Yapay Zekâ.

ABSTRACT
MS THESIS
SMART INTRUSION DETECTION SYSTEMS

Hanifi TOPRAK

**THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE OF BATMAN
UNIVERSITY
THE DEGREE OF MASTER OF SCIENCE
IN ELECTRICAL AND ELECTRONIC ENGINEERING**

Advisor: Assoc. Prof. Dr. Süleyman KARDAŞ

2021, 88 Pages

Jury

**Advisor Assoc. Prof. Dr. Süleyman KARDAŞ
Assoc. Prof. Dr. Ömer Faruk ERTUĞRUL
Assoc. Prof. Dr. Cafer BUDAK**

Information and Communication Technologies have become an inseparable part of the people who take every part of our lives. This is expected to increase in our lives. It is natural for those who want to use it for their own purposes because of the fact that technology is so intertwined with our lives. In case of not taking necessary precautions against the many benefits of technology, it can cause irreparable results with the effect of others. In particular, attackers try to infiltrate or become useless in systems such as Banking, Energy, and Transportation, which are the most influential areas of society. For the attacker, motivation can sometimes be Money and sometimes glory. It is a fact that everyone has accepted that there is a security problem everywhere. For this reason, the USOM has been established across the country for total cyber-wars, while institutions are creating their own cyber-incident intervention teams (SOME).

A cyber attack is an assault launched by cybercriminals using one or more devices against a single or multiple devices or networks. A cyber attack can disable system, steal data, or alter data. Cyber attackers apply to various technical and social engineering ways to access the target system(s). Intrusion Detection Systems (IDS) is one of the security components used to detect potential attacks. IDS systems generally try to detect attacks in 3 different ways. **Signature Based IDS:** This intrusion detection system compares the existing malware database with any abnormalities in the network. **Anomaly Based IDS:** User profiles are created in this intrusion detection system. It is interpreted as an attack in case of going out of these profiles. **Protocol Analysis IDS:** Protocol activities are profiled. When a suspicious activity is encountered, it is compared to existing profiles.

KDD'99: KDD'99 is a data set used to design models for intrusion detection systems. This data set consists of 42 columns and 4,9402,000 rows. The attack in the data set can be defined in 4 main categories. **DoS:** denial-of-service is the rendering of a device on the network that cannot serve real users by consuming system resources.

Example attack: syn flood. **R2L**: Attempt to connect to a system without access. Example attack: guessing password. **U2R**: It is the attack type to obtain admin or root user rights while having normal user rights. Example attack: buffer overflow. **Probing**: This attack collects information about the target device. This information includes open ports, valid IP addresses, services running on it, operating system installed, and so on. Example attack: port scanning.

In this thesis, the attacks in the KDD'99 data set used in Intrusion Detection systems will be categorized and attack statistics and information about these attacks will be given. In addition, system models that will detect an attack that can be performed by using Artificial Neural Networks (ANN) and Decision Tree algorithms, which are among the supervised learning models, have been made in real time and with high performance.

Keywords: Artificial Intelligence, Artificial Neural Networks, Cyber Security, Decision Trees, Intelligent Attack Detection Systems, KDD'99

ÖNSÖZ

Bu tez çalışmamda, bilgi ve tecrübelerini çözüm odaklı bakış açısıyla bana aktaran; her zaman yanımda olan değerli danışmanım Dr. Öğr. Üyesi Süleyman KARDAŞ'a teşekkür ederim.

Bilgi ve birikimiyle her zaman bana yol gösteren, akademik duruşuyla örnek olan değerli hocam Prof. Dr. Murat KAYRI'ye teşekkürü bir borç bilirim.

Gerek ders aşaması gerekse tez yazım aşamasında ihtiyaç duyulan zamanda yardımlarını esirgemeyen değerli hocalarım Doç. Dr. Ömer Faruk ERTUĞRUL, Dr. Öğr. Üyesi Ramazan TEKİN, Dr. Öğr. Üyesi Emrullah ACAR ve Dr. Öğr. Üyesi Abidin ÇALIŞKAN'a teşekkür ederim.

Maddi ve manevi olarak her zaman yanımda olan beni büyüterek bugünlere getiren anneme ve desteklerini her daim hissettiğim canım eşime ve çocuklarıma sabır ve fedakârlıklarından ötürü çok teşekkür ederim.

Hanifi TOPRAK
BATMAN-2021

İÇİNDEKİLER

ÖZET	I
ABSTRACT	iii
ÖNSÖZ	v
İÇİNDEKİLER	vi
ŞEKİLLER TABLOSU	viii
TABLolar LİSTESİ	x
SİMGELER VE KISALTMALAR	xi
1. GİRİŞ	1
1.1 Siber Güvenlik	3
1.2.1 Siber Tanımı	3
1.2.2 Siber Güvelik	3
1.2.3 Siber Saldırı	4
1.2.4 Saldırı Tespit Sistemleri	4
1.2 Saldırı Tespit Sistemleri	5
1.2.1 Saldırı Tespit Sistemi	5
1.3 Saldırı Önleme Sistemleri	6
1.4 Yapılan Büyük Çaplı Saldırıları	7
1.4.1 Wannacry	7
1.4.2 Notpetya/Expetr	7
1.4.3 Stuxnet	7
1.4.4 Darkhotel	8
1.4.5 Mirai	8
1.5 USOM	8
1.6 Kurumsal SOME	8
1.7 OSI Referans Modeli	9
1.7.1 OSI (Open System Interconnection)	9
1.8 Saldırı Tespit Sistemlerinde Kullanılan Veri Setleri	11
1.8.1 DARPA (Lincoln Laboratuvarı – 1998/1999)	11
1.8.2 KDD’99 (Massachusetts Teknoloji Enstitüsü– 1998/1999)	11
1.8.3 DEFCON (Shmoo Grup, 200/2002)	11
1.8.4 CAIDA (Uygulamalı İnternet Veri Analiz Merkezi, 2002/2016)	12
1.8.5 LBNL (Lawrence Berkeley National Laboratory Ve ICSI 2004-2005)	12
1.8.6 CDX (United States Military Academy 2009)	12

1.8.7	Kyoto (Kyoto University 2009).....	13
1.8.8	Twente (University of Twente 2009).....	13
1.8.9	UMASS (University of Massachusetts 2011)	14
1.8.10	ISCX2012 (University of New Brunswick 2012)	14
1.8.11	ADFA (University of New SouthWales 2013).....	14
2.	KAYNAK ARAŞTIRMASI	15
3.	MATERYAL VE YÖNTEM.....	18
3.1	Materyal	18
3.1.1	KDD'99.....	18
3.1.1.1.	Saldırı Tipleri.....	26
3.1.1.2.	Eliminasyon İşlemi	30
3.1.1.3.	KDD Veri Setine Eklenen Çıkış Değişkenleri.....	31
3.1.1.4.	Bağımsız Değişkenlerin Sonuç Üzerindeki Etkileri	31
3.2	Yöntem	34
3.2.1	Öğrenme Algoritmaları.....	36
3.2.1.1.	Gözetimli-Eğitilmiş-Denetimli Öğrenme (Supervised Learning)	36
3.2.1.2.	Gözetimsiz-Eğitimsiz-Denetimsiz Öğrenme (UnSupervised Learning)	36
3.2.1.3.	Kullanılan Algoritmalar	38
4.	ARAŞTIRMA SONUÇLARI VE TARTIŞMA.....	44
5.	SONUÇLAR VE ÖNERİLER.....	79
6.1	Sonuçlar	79
6.2	Öneriler.....	80
6.	KAYNAKÇA	82
	ÖZGEÇMİŞ.....	87

ŞEKİLLER TABLOSU

Şekil 1.1. Veri seti oluşturulurken kullanılan ağ yapısı (Anonymous, 2020).	13
Şekil 3.1. C5.0 ve YSA Tekniğini Kullanarak Model Geliştirme ve Test Etme Süreci (Pratibha Soni ve ark., 2014).	15
Şekil 3.2. JAVA-ML Kütüphanesi ile özellik seçimi (Harbora ve ark., 2014)	16
Şekil 4.1. KDD'99 veri seti ham hali.....	19
Şekil 4.2. Üst Sınıflara göre kategorize edilmiş saldırı istatistikleri	24
Şekil 4.3 Tekrarlı verinin eleme işlemi.	31
Şekil 4.4. Uygulanan sistem mimarisi.....	35
Şekil 4.5. YSA Çalışma Prensibi (Jain, 2016).	38
Şekil 4.6. Bir nöronun yapısı (Jain, 2016).....	39
Şekil 4.7. Karar Ağacı Modeli	41
Şekil 5.1. YSA Levenberg-Marquard öğrenme algoritması plot regresyon grafiği	45
Şekil 5.2. YSA Bayesian Regularization öğrenme algoritması plot regresyon grafiği	45
Şekil 5.3. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 10 gizli katmanlı (0:Saldırı Değil, 1:Saldırı)	48
Şekil 5.4. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 15 gizli katmanlı (0:Saldırı Değil, 1:Saldırı)	49
Şekil 5.5. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 30 gizli katmanlı (0:Saldırı Değil, 1:Saldırı)	49
Şekil 5.6. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 50 gizli katmanlı (0:Saldırı Değil, 1:Saldırı)	50
Şekil 5.7. Eliminasyon sonrası Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 10 gizli katmanlı (0:Saldırı Değil, 1:Saldırı)	53
Şekil 5.8. Eliminasyon sonrası Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 15 gizli katmanlı (0:Saldırı Değil, 1:Saldırı).	53
Şekil 5.9. Eliminasyon sonrası Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 30 gizli katmanlı (0:Saldırı Değil, 1:Saldırı)	54
Şekil 5.10. Eliminasyon sonrası Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 50 gizli katmanlı (0:Saldırı Değil, 1:Saldırı).	54
Şekil 5.11. Saldırı Çıktısına ait plot regresyon grafiği (satan, neptune, vb).....	56
Şekil 5.12. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, (0:Saldırı Değil, 1:Saldırı). ..	56
Şekil 5.13. Saldırı türüne ait doğruluk ve karışıklık matrisi, (1:DoS, 2: R2L, 3:Probe, 4:U2R, 5: Normal Bağlantı).....	57

Şekil 5.14. DoS saldırısı ait doğruluk ve karışıklık matrisi (0: DoS Saldırı Değil,1:DoS Saldırısı).....	58
Şekil 5.15. Probe saldırısı ait doğruluk ve karışıklık matrisi (0: Probe Saldırı Değil,1:Probe Saldırısı)	
.....	59
Şekil 5.16. R2L saldırısı ait doğruluk ve karışıklık matrisi (0: R2L Saldırı Değil,1: R2L Saldırısı)....	59
Şekil 5.17. U2R saldırısı ait doğruluk ve karışıklık matrisi (0: U2R Saldırı Değil,1: U2R Saldırısı) .	60
Şekil 5.19. 10 Gizli Katmanlı YSA Modeli.	61
Şekil 5.20. Saldırı çıktısına ait plot regresyon grafiği (satan, neptune, vb).	63
Şekil 5.21. Saldırı olup olmadığına ait plot regresyon grafiği (Evet,Hayır).	63
Şekil 5.22. Saldırı tipine ait plot regresyon grafiği (DoS, Probe, U2R ve R2L).....	64
Şekil 5.23. DoS saldırısı Olup Olmadığına ait plot regresyon grafiği (Evet,Hayır).	64
Şekil 5.24. Probe saldırısı Olup Olmadığına ait plot regresyon grafiği (Evet,Hayır).	65
Şekil 5.25. R2L saldırısı Olup Olmadığına ait plot regresyon grafiği (Evet,Hayır).	65
Şekil 5.26. U2R saldırısı olup olmadığına ait plot regresyon grafiği (Evet,Hayır).....	66
Şekil 5.27 30 Gizli Katmanlı YSA Modeli.	66
Şekil 5.28. Saldırı çıktı değerine ait hata matrisi (1=Evet, 0=Hayır).	70
Şekil 5.29. Saldırı çıktı değerine ait ROC Eğrisi.	70
Şekil 5.30. Saldırı Üst Türüne ait hata matrisi (Dos, Probe vb.).....	71
Şekil 5.31. Saldırı Üst Sınıf saldırı türüne(DoS, U2R,R2L,Probe) ait ROC Eğrisi.	71
Şekil 5.32. DoS Saldırısına ait hata matrisi (1=Evet, 0=Hayır).	72
Şekil 5.33. DoS saldırı türüne ait ROC Eğrisi.....	72
Şekil 5.34. R2L Saldırısına ait hata matrisi (1=Evet, 0=Hayır).	73
Şekil 5.35. R2L Saldırı türüne ait ROC eğrisi.....	73
Şekil 5.36. Probe Saldırısına ait hata matrisi (1=Evet, 0=Hayır).	74
Şekil 5.37. Probe saldırı türüne ait ROC eğrisi.	74
Şekil 5.38. U2R Saldırısına ait hata matrisi (1=Evet, 0=Hayır).....	75
Şekil 5.39. U2R Saldırı türüne ait ROC eğrisi.	75
Şekil 5.40. Saldırı çeşidine ait hata matrisi (satan, neptune, vb.).....	76
Şekil 5.41. Saldırı Çeşidine (Satan, neptune, vb.) ait ROC eğrisi.....	76

TABLÖLER LİSTESİ

Tablo 1.1. Stuxnet saldırısında etkilenen bilgisayarların ülkelere göre oranı	7
Tablo 2.1. Doğruluk oranı (Obeida ve ark.,2019).....	17
Tablo 3.1. TCP bağlantısının temel özellikleri	20
Tablo 3.2. Bağlantıya ait içerik özellikleri	20
Tablo 3.3. İki saniyelik zaman içerisinde elde edilen trafik özellikleri	21
Tablo 3.4. İki saniyeden uzun saldırılarda ana bilgisayar özellikleri.....	21
Tablo 3.5. KDD veri setindeki kategorize edilmiş ataklar.....	22
Tablo 3.6. KDD veri setindeki saldırıların numerik karşılığı ve eklenen Üst sınıf Verisi.....	23
Tablo 3.7. KDD'99 Veri setinin %10'luk dilimindeki saldırılar ve yüzdeleri.	24
Tablo 3.8. KDD'99 Veri seti tekrarlı verinin elenmesi sonrası saldırılar ve yüzdeleri	26
Tablo 3.9. Bağımsız değişkenin bağımlı değişken üzerindeki etkisi.....	32
Tablo 4.1. Levenberg-Marquard Bayesian Regularization Karşılaştırılması	44
Tablo 4.2. Farklı Gizli Katman Sayılarıyla Sonuçların Karşılaştırılması	47
Tablo 4.3. Eliminasyon sonrası elde edilen sonuçlar.....	52
Tablo 4.4. 10 Gizli Katmanlı ve Farklı Çıkış Parametresine Göre Sonuçlar.....	55
Tablo 4.5. 30 Gizli Katmanlı ve Farklı Çıkış Parametresine Göre Sonuçlar.....	62
Tablo 4.6. Decision Trees algoritması test sonuçları.....	68
Tablo 4.7. Bu çalışmadaki sonuçlar ile farklı yaklaşımların karşılaştırılması.	77

SİMGELER VE KISALTMALAR

YSA	: Yapay Sinir Ağları
STS	: Saldırı Tespit Sistemleri
IDS	: Intrusion Detection Systems
ANN	: Artificial Neural Network
DT	: Decision Tree
SVM	: Support Vector Machines
KNN	: K-Nearest Neighbors
SIEM	: Security Information and Event Management – Bilgi güvenliği Tehdit ve Olay Yönetimi
DoS	: Denial of Services
U2R	: User to Root
R2L	: Remote to Local
IPS	: Intrusion Prevent Systems
SÖS	: Saldırı Önleme Sistemleri
UTM	: Unified Threat Management
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
SOME	: Siber Olaylara Müdahale Ekibi
OSI	: Open System Interconnection
IP	: Internet Protocol
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
DHCP	: Dynamic Host Configuration Protocol
SSH	: Secure Shell
FTP	: File Transfer Protocol
SNMP	: Simple Network Management Protocol
HTTP	: Hypertext Transfer Protocol
DNS	: Domain Name System
KDD	: Knowledge Discovery Database
URL	: Uniform Resource Locator
SYN	: Synchronize

ACK	: Acknowledge
ICMP	: Internet Control Message Protocol
MTU	: <i>Maksimum</i> Transfer Unit
IBM	: International Business Machines
SPSS	: Statistical Package for the Social Sciences
FLDA	: Fisher Linear Discriminant Analysis
MATLAB	: Matrix Laboratory
ROC	: Receiver Operating Characteristic
AUC	: Area Under Curve

1. GİRİŞ

Her geçen gün hızla gelişen bilişim teknolojileri, insanların internet kullanıcısı olmasını zorunlu duruma getirmiştir. Dünya nüfusunun yaklaşık %56'sı (4,38 Milyar) internet kullanıcısıdır (Bayrak, 2019). İnternet kullanımında bu oranda bir artışın olması internetin hayatı kolaylaştırması ve özgürleştirmesinden kaynaklıdır. Ancak bu faydalarla birlikte internetin kişileri ve sistemleri hedef haline getirmesi gibi dezavantajları da beraberinde getirmektedir. İnternete bağlı bir sistem ya da kullanıcı hedef durumuna düşebilmektedir. Siber saldırı, hedef sistemlerin erişilebilirlik, bütünlük veya gizliliğine karşı yapılan, kişi veya kişiler tarafından yapılan işlemdir (Anonim, 2016). Her geçen gün dünya üzerinde yapılan siber saldırı türleri ve sayısı artmaktadır. Bununla beraber yapılan güncelleme ve yamalar ile bazı saldırı türlerinde düşüşler meydana gelebilmektedir. Örneğin bulaştığı sistemlerin dosyalarını kriptolayıp dosya şifrelerinin çözülmesi karşılığında ücret isteyen Ransomware (Fidye) yazılımları, 2015 yılı içerisinde 3,8 milyon, 2016 yılı içerisinde 538 milyon ve 2017 yılı içerisinde 183,6 milyon saldırı Sonicwall tarafından tespit edilmiştir (Anonim, 2018). Bu fidye yazılımından, 2016 yılında yüksek sayıda saldırı yapılmışken iken 2017 yılında bu saldırı türünde düşüş meydana gelmesinin sebebi bu saldırı çeşidine karşı geliştirilen önlemler olmuştur. Bunu gören saldırganlar farklı saldırı türlerine yönelmiştir. Siber saldırılar, kurum bilgi varlıkları için hayati bir öneme sahiptir (Khadraoui ve ark., 2017). Kurumsal yapılarda kurum dışından yapılacak siber saldırıların önlenmesi için güvenlik duvarları ve SIEM (Security Information and Event Management – Bilgi güvenliği Tehdit ve Olay Yönetimi) yazılımlar üzerinde gerekli yapılandırmalar yapılarak sistemler korunaklı hale getirilmesi mümkündür.

Siber saldırı, bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, herhangi bir yerdeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemleri tanımlamaktadır (Anonim, 2016). Siber Salırganlar hedef sisteme erişmek için türlü yola başvururlar. Ağa dahil olan cihaz sayısı arttıkça ağın güvenliğini sağlamak da o derece zorlaşmaktadır (Aggarwal ve ark. S, 2015). Saldırı tespit sistemleri (Intrusion Detection Systems), olası atakları tespit etmekte kullanılan güvenlik bileşenlerinden biridir (Jayshree ve ark., 2012). IDS sistemleri yapılan atakları genel olarak 3 farklı şekilde tespit etmeye çalışır. Bunlar:

İmza Tabanlı STS: Bu saldırı tespit sisteminde, ağda oluşabilecek anormallik mevcut kötü yazılım veri tabanı ile karşılaştırma yapılarak tespit edilmeye çalışılır.

Anomali Tabanlı STS: Ağda geçen paketlerin başlık bilgileri alınır ve ilgili makinenin daha önceki davranışları ile karşılaştırılır. Bir anormallik görülmesi durumunda alarm üretilir.

Protokol Analizi STS: Protokol aktiviteleri profilleri çıkarılır. Şüpheli bir aktivite ile karşılaşıldığında mevcut profillerle karşılaştırılır.

İmza Tabanlı STS yeni saldırıları tespit edemediğinden güvenlik zafiyetine neden olmaktadır. Bundan dolayı güvenliği üst seviyede tutan kurum ve kuruluşlar bunun yanında Anomali tabanlı STS ve Protokol Analizi tabanlı STS'leri kullanmaktadırlar. Kullanılan STS'ler kullanılan algoritmanın güçlülüğüne göre farklı oranlarda yanlış alarmlar üretmektedir. STS'lerde hedef, bu yanlış alarmları minimize ederken gerçek saldırıyı tespit etmektir. Ağ üzerindeki saldırılar dört farklı şekilde yapılır (Erol, 2005). Bu yöntemler sırasıyla;

- **Bilgi Tarama-Probe:** Bu saldırı türünde, hedef cihaz ya da cihazlar hakkında veri elde etme amacı güdülmektedir (Tanrıku ve ark., 2009). Bilgi tarama teknikleri ile hedef cihazın işletim sistemi, açık portları, IP adresi gibi bilgiler elde edilmeye çalışılır.
- **Denial of Service DoS- Hizmet Engelleme:** Hedef sisteme, saldırgan tarafından gönderilen paketlerle hizmet veremez duruma gelmesidir. DoS saldırılar farklı türleri bulunmaktadır (Hussain ve ark, 2004).
- **Remote to Local-Yönetici Hakları ile Oturum Açma:** Kullanıcı Haklarına sahip olmadığı halde hedef sistemde oturum açma saldırılarıdır (Erol, 2005).
- **User to Local – Kullanıcı Hak Yükseltme:** Normal kullanıcı hakkına sahipken yönetici hakkına yükseltme dayalı bir saldırı türüdür.

Akıllı saldırı tespit sistemlerinin temel prensibi verinin işlenip karşılaşılabilecek yeni bir bağlantı için karar vermesini sağlamaktır. Karar verme sürecinde verilen kararın doğru karar olması önem arz etmektedir.

Heba F. Eid ve ark., (2010), KDD'99 veri seti üzerinde, Temel Bileşen Analizi (Principal Component Analysis- PCA) ile Destek Vektör Makineleri (Support Vector Machines- SVMs) kullanarak en uygun modeli ortaya koymuşlardır.

Pratibha Soni ve ark., (2014), çalışmalarında KDD'99 veri setinin %10'luk dilimi kullanmıştır. Çalışmalarında Karar Ağaçları ve Yapay Sinir Ağları yöntemleri ile özelliklerin modelin başarı üzerindeki etkisini ortaya koymuşlardır. Eğitim ve test veri setlerinin değişik parametrelere ile deneyerek DoS, R2L, U2R ve Probe saldırısını tespit etme ve doğruluk oranları belirlemişlerdir. U2R ve Probe saldırıları için %70 Eğitim ve %30 Test veri seti olarak

uygulandığında sırasıyla %99,99 ve %99,94 doğruluk oranlarına ulaşmışlardır. DoS ve R2L saldırıları için %70 Eğitim ve %30 Test veri seti olarak uygulandığında sırasıyla %99,94 ve %99,92 doğruluk oranlarına ulaşmışlardır.

Harbora ve ark., (2014), KDD'99 veri setinin %10 luk dilimini veri madenciliği algoritmalarını test etmek için kullanmışlardır. Veri ilişkilendirme kuralları, ön işleme, regresyon, sınıflandırma, kümeleme, ilişkilendirme kuralları ile görselleştirme için algoritma ve araçlarını barındıran WEKA kullanılmıştır.

Obeida ve ark., (2019), KDD'99 veri seti üzerinde J48, Random forest, Random Tree, Decision Table, Multilayer Perceptron (MLP), Naïve Bayes ve Bayes Network sınıflandırma algoritmaları kullanılarak çıkan sonuçları karşılaştırmışlardır. %93,75 başarı yüzdesi ile en iyi sonuç Random forest algoritması ile elde etmişlerdir.

Bu tezde, saldırı tespit sistemleri için oluşturulmuş KDD'99 veri seti kullanılarak Yapay Sinir Ağları ve Karar Ağaçları tabanlı gerçek zamanlı çalışan saldırı tespit yöntemleri geliştirmiştir. Ağdaki paketin mevcut modelin öğrenmesinden yola çıkarak saldırı olup olmadığı, saldırı ise hangi üst saldırı türü (DoS, Probe, U2R ve R2L) olduğu ve bununla birlikte hangi saldırı (Satan, neptune, nmap ftp_write vb.) olduğu ortaya konulmaktadır.

Yapılan çalışmada da görüleceği üzere, bazı parametrelerin modele dâhil edilmemesi modelin karmaşıklığını azalttığı ayrıca gelen paketin saldırı olup olmadığı, saldırı türünü açıklamada diğer önceki çalışmalardan daha iyi sonuç verdiği görülecektir.

1.1 Siber Güvenlik

1.2.1 Siber Tanımı

Siber kelimesi “sibernetik” kökünden gelmektedir. Sibernetik ise kendi kendine denge kurarak kontrol etme ve yönetme anlamındadır. İnsan yaşamı ile makinelerin yönetişimi şeklinde birbirleri ile bilgi alış-verişi olarak “Siber” terimi tanımlanabilir (Ünaldı, 2003). Günümüzde ise daha çok sanal erişim veya sanal yaşam olarak kullanılmaktadır.

1.2.2 Siber Güvelik

Siber saldırılara karşı alınacak topyekûn önlemlerdir. Saldırganlar, hedef sistem, kurum ya da kişiye çeşitli yöntemlerle saldırı gerçekleştirmektedir. Siber saldırırganlar sistemlerin normal iş süreçlerini kesmek ya da yavaşlatmak isterler (Anonymous, 2020). Siber saldırırganların bir diğer hedefi ise hedef sistemlere sızmaştır (Saravan ve ark., 2019). Siber

saldırılarından korunmak için başarılı bir siber güvenlik yaklaşımına ihtiyaç vardır. Bu yaklaşımda birden fazla katman bulunmaktadır. Bir kurum veya kuruluşta, bir bütün olarak saldırılara karşı önlemler alınabilir. Çalışanlar ve teknolojik alt yapı birbirini tamamlamalıdır (Anonim, 2020).

1.2.3 Siber Saldırı

Siber saldırı, bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, herhangi bir yerdeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemleri tanımlamaktadır (Anonim, 2016). Siber Saldırganlar hedef sisteme erişmek için türlü yola başvururlar. Ağa bağlanan cihazlar arttığı için ağın güvenliğini sağlamak da o derece zorlaşmaktadır (Aggarwal ve ark., 2015).

Hedef sistem üzerinde saldıran kişi veya kişilerin amaçlarını elde etme için yapılan girişime verilen addır. Hedef sistemin çalışmasını durdurma ya da hedef sistemden veri çalma gibi amaçlar güdülebilir. Siber saldırılar iki türdür. Bunlar Aktif ve Pasif saldırılar olarak tanımlanır. Aktif saldırıda saldırgan, sistem kaynaklarını değiştirmeye veya işlemez hale getirmeye çalışır (DoS vb.). Pasif saldırıda ise saldırgan, hedef sistemden bilgi almaya ya da yararlanmaya çalışır. Sistem kaynaklarında herhangi bir değişiklik yapılmaz. Veri hırsızlığı bu saldırı türüne girer.

1.2.4 Saldırı Tespit Sistemleri

1.1.4.1. Güvenlik Duvarı

Mevcut network içerisinde içeriden dışarıya ve dışarıdan içeriye gelen trafiği kontrol eden ve uygulanan politikalara göre trafiği kesen ya da geçişine izin veren güvenlik bileşenidir. Firewall kendisine gelen paketleri gönderilen yere gitmesinin üzerindeki kurallara göre gitmesine izin verir ya da düşürür (Anonim, 2020)

1.1.4.2. Antivirüs Yazılımları

Kurulu olduğu cihazı, virüslere karşı koruyan yazılımlara verilen addır. Antivirüs yazılımlar ilk ortaya çıktığında sadece cihazı bilgisayar virüslerine karşı korumakla görevli iken sonraları tarayıcı güvenliği, fidye yazılımları, tuş kaydedici, arka kapı açıkları, tojen, enfekte olmuş URL gibi sorumluluklar da almıştır.

Antivirüs yazılımları virüs tespitini aşağıdaki yöntemlerle yapmaktadırlar.

İmza Tabanlı Algılama: Geleneksel anti-virüs yazılımların sıklıkla başvurduğu yöntemdir. Öncelikle anti-virüs yazılımı üreticisi tespit ettiği yazılımın kötü ya da iyi olduğunu tespit etmek için ilgili yazılımı incelemeye alırlar. Kötü olarak analiz edilen yazılımın bir imzası oluşturulmakta ve bu imzalar ilgili üreticinin uygulamasını kullanan istemcilere gönderilir. Dolayısı ile client bahse konu yazılım ile karşılaştığında imza veri tabanında ilgili yazılımın virüs olduğu bilgisi olduğunda yazılımı engelleme işlemi yapılır. İmza tabanlı algılamada hata payı minimumdur. Fakat bu yöntemde anti-virüs yazılımın güncel olması büyük önem arz etmektedir.

Sezgisel Algılama: Zararlı yazılım bulaştığı bir sistemde ya da cihazda mutasyona uğrayıp farklı şekiller alabilmektedir. Bu durumda imza tabanlı algılama yöntemi ile virüsün tespiti mümkün olamamaktadır. Anti-virüs yazılımı virüsün ilk halinden yola çıkarak virüs olduğunu tespit etme yöntemidir.

Rootkit Algılama: Rootkit, işletim sistemleri çekirdeklerine yetkisiz olarak ulaşarak cihazın uzaktan kontrolü sağlamasına neden olan kötü niyetli yazılımlara verilen addır (Anonim, 2020). Anti-virüsler rootkitleri tarama işlemini yaparlar. Bu işlem yapıldığında virüsün tespiti yapılabilir. Bu algılama yöntemine rootkit algılama denilmektedir.

Gerçek Zamanlı Algılama: Bilgisayarın belleğinde yürütülen işlemlere bakarak algılama yapma yöntemidir.

1.2 Saldırı Tespit Sistemleri

1.2.1 Saldırı Tespit Sistemi

Saldırı tespit sistemi (İngilizce: Intrusion Detection Systems IDS) ilk olarak 1980 yılında James P. Anderson tarafından geliştirilmiştir. 1980-90 yılları arasında birçok araştırmacı bu konu hakkında ABD tarafından desteklenmiştir (Bruneau, 2020). İlk saldırı tespit sistemi 1984-86 yılları arasından Dorothy Denning ve Peter Neumann tarafından geliştirilmiş ve bu gerçek zamanlı saldırı tespit sistemlerinin ilkidir (Bruneau, 2020). Bu saldırı sistemi Saldırı Tespit Uzman Sistemi (İngilizcesi Intrusion Detection Expert System, IDES) olarak isimlendirilmiştir.

Saldırı tespit sistemleri (Intrusion Detection Systems) IDS, olası atakları tespit etmekte kullanılan güvenlik bileşenlerinden biridir (Jayshree ve ark., 2012). IDS sistemleri yapılan atakları genel olarak 3 farklı teknik ile tespit etmeye çalışır. Bunlar:

1.2.2.1 İmza Tabanlı STS

Bu saldırı tespit sisteminde ağda oluşabilecek anormallik mevcut kötü yazılım veri tabanı ile karşılaştırma yapılır.

1.2.2.2 Anomali Tabanlı STS

Ağda geçen paketlerin başlık bilgileri alınır ve ilgili makinenin daha önceki davranışları ile karşılaştırılır. Bir anormallik görülmesi durumunda alarm üretilir.

1.2.2.3 Protokol Analizi STS

Protokol aktiviteleri profilleri çıkarılır. Şüpheli bir aktivite ile karşılaşıldığında mevcut profillerle karşılaştırılır.

İmza Tabanlı STS yeni saldırıları tespit edemediğinden güvenlik zafiyetine neden olmaktadır. Bundan dolayı güvenliği üst seviyede tutan kurum ve kuruluşlar bunun yanında Anomali tabanlı STS ve Protokol Analizi STS leri kullanmaktadırlar. Kullanılan STS'ler kullanılan algoritmanın güçlülüğüne göre farklı oranlarda yanlış alarmlar üretmektedir. STS'lerde hedef, bu yanlış alarmları minimize ederken gerçek saldırıyı tespit etmektir.

Saldırı Tespit Sistemleri, sistemlere veya networklere yapılan kötü niyetli aktivitelere karşı korumak için geliştirilen güvenlik bileşenlerinden bir tanesidir. Günümüz şartlarında bir ağın ya da sistemin güvenliğini geleneksel yöntemlerle tek başına sağlamak güç bir durumdur.

1.3 Saldırı Önleme Sistemleri

Saldırı tespit sistemleri tarafından tespit edilen kötü niyetli aktivitelere yönelik alınan önlemler bütünüdür.

Saldırı Tespit Sistemleri (IDS) tespit edilen saldırıları raporlar ve gerekli yerlere alarm üretirken Saldırı Önleme Sistemleri (IPS) ise tespit edilen saldırıyı önlemeye yönelik işlem yaparlar.

Gelişen teknolojik atılımlarla sadece güvenlik duvarı sistemlerin ve networklerin güvenliğini sağlamada yetersiz kaldığı herkesin malumudur. Güvenlik duvarları üzerindeki kurallara göre gelen-giden paketi düşürür ya da geçişine izin verir. Fakat iç networkte yapılan bir saldırının güvenlik duvarı tarafından tespiti mümkün olmamaktadır. Dolayısı ile networkün güvenliğinin sağlanması için Güvenlik Duvarı, Saldırı Tespit Sistemi ve Saldırı Önleme Sistemleri birlikte kullanılması gerekmektedir.

Son yıllarda yukarda bahsedilen Saldırı Tespit Sistemleri (IDS), Saldırı Önlemleri Sistemleri ve Güvenlik Duvarı gibi güvenlik bileşenleri tümleşik sunulmaktadır. Bu tarz yapılar Unified Threat Management (UTM) olarak tanımlanmaktadır. Bu da eski tarz güvenliğin çok ötesinde çözümler sunmaktadır.

1.4 Yapılan Büyük Çaplı Saldırıları

Kaspersky'ye göre son on yılda gelmiş geçmiş en büyük saldırılar aşağıda listelenmiştir.

1.4.1 Wannacry

Windows İşletim sistemin bir açığına sömürerek yapılan bir saldırdır. Saldırı iki etapta oluşmaktadır. Öncelikle virüs hedef cihaza indirilip başka makinelerle bulaştırılma işlemi yapılmakta ikinci bölümde ise fidye yazılımı indirilerek tüm dosyaları şifrelenmektedir. Microsoft firması bahsedilen açığı 14. Mart 2017 tarihinde yayınladığı güncelleme ile kapatmıştır. Bu saldırıdan 150 ülkeden en az 200.000 cihaz etkilenmiştir (Perekarin, 2017).

1.4.2 Notpetya/Expetr

Wannacry gibi bu solucan da Windows işletim sisteminin Eternalblue açığını kullanarak sistemlere enjekte olmaktadır. Çalışma mantığı olarak Wannacry ile aynıdır. Tek farkları şifrelenen dosyalar Wannacry'da geri getirilebilirken Notpetya'da geri dönülemez şekilde dosyalar şifrelenmektedir. Bu da bu veridiği hasar olarak Wannacry'ı geride bırakmaktadır. Bu salgının verdiği toplam zarar 10 milyar dolar civarında olduğu belirtilmektedir (Mcquade, 2018).

1.4.3 Stuxnet

İranın nükleer çalışmalarını baltalamak üzere yapılan siber saldırıdır. İrana ait Buşehr ve Natanz şehirlerinde bulunan nükleer reaktörler etkilenmiştir. Stuxnet saldırısı, kapalı devre sistemlerin de hedef olabileceğini göstermesi açısından önem arz etmektedir. Stuxnet solucanında etkilenen ülkelerin oranı aşağıdaki tabloda belirtilmiştir (Anonim, 2017).

Tablo 1.1. Stuxnet saldırısında etkilen bilgisayarların ülkelere göre oranı

Ülke	Etkilenen Bilgisayar Oranı
İran	58,85%
Endonezya	18,22%
Hindistan	8,31%
Azerbaycan	2,57%
Amerika Birleşik Devletler	1,56%
Pakistan	1,28%
Diğer Ülkeler	9,20%

1.4.4 Darkhotel

Darkhotel saldırısı, otelde misafir olan üst düzey yöneticilere yönelik bir saldırdır. Bu saldırıda otelde kalan misafirler ağı bağlandığında herkesçe çok kullanılan bir uygulamanın güncellenmesi yapılmış gibi izlenim uyandırılır ancak burada zararlı yazılımın cihaza indirilmesi hedeflendirilir. Hedef cihaza zararlı yazılım yüklendikten sonra arka kapı açılarak cihazdaki gizli veriler dışarıya aktarılır. Darkhotel virüsünün kaynağı olarak Kuzey Kore gösterilmektedir (Anonim, 2020).

1.4.5 Mirai

Nesnelerin interneti olayının ortaya çıkması ile ağı dahil olan ve güvenliği sağlanmayan çok sayıda cihaz ortaya çıktı. Bu cihazlara kameralar ve DVR cihazları örnek verilebilirler (Woolf, 2016). Güvenlik sağlanmadan ağı katılan bir cihazı tespit eden saldırgan kamera ve DVR cihazlarına virüs bulaştırıp zombi ağlarına dahil ederler. 21 Ekim 2016 tarihinde DNS servis sağlayıcısı DYN sunucularına istekte bulunuldu. DYN bu isteklere cevap veremeyecek duruma gelmiş DNS hizmeti verilememiştir. Bu saldırı ile akıllı cihazların güvenliğinin önemi ortaya çıkmıştır.

1.5 USOM

20 Haziran 2013 yılında ülkemize yönelik yapılmış siber saldırıların tespit edilmesi, yapılacak olanların bertaraf edilmesi ve etkilerinin azaltılmasına yönelik Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) kurulmuştur (Anonim, 2013). USOM, Uluslararası ve ülke içinde sanal ortamda öngörülen tehditlerle ilgili kendisine ulaşan bildirimleri yorumlar ve boşa çıkarmak için Kamu Kurumları ve Özel Sektörle iletişim halinde olur. Bu bağlamda kendisine ulaşan bildirim ile ilgili çözümleme ve sonuçlandırma işlemini yürütür ve takipçisi olur (Anonim, 2013). Aynı zamanda yurt içi ve yurt dışı tatbikatlar yaparak yurttaki siber saldırılara yönelik farkındalık yaratır.

1.6 Kurumsal SOME

Siber Olaylara Müdahale Ekibinin kısaltılmış halidir. Kurumlarına yapılan veya yapılması planlanan siber saldırılara yönelik önlem alma, gerektiğinde USOM ile iletişime geçmekle yükümlüdürler. Kurumsal SOME'ler, kurumların teknik alt yapı ve idari kısımlarında siber güvenlik konusunda önerilerde bulunurlar. Kurumsal SOME; Bakanlıklar, Müstakil Kamu Kurumları ve Bilgi İşlem birimine sahip kamu kurumlarından oluşmaktadır. USOM tarafından verilen görevleri yapmakla mükelleftir (Anonim, 2017).

Bilgi İşlem birimi olan kamu kurum ve kuruluşları veya kritik alt yapı işleten özel sektör Kurumsal SOME içerisinde yer almaktadır (Anonim, 2014).

1.7 OSI Referans Modeli

1.7.1 OSI (Open System Interconnection)

ISO aynı networkteki cihazların birbirleri ile olan iletişimi nasıl olacağı ile ilgili kuralları OSI modelinde tanımlamaktadır. 1984 senesinde OSI referans modeli olarak yayınlanmıştır. OSI referans modeli öncesi aynı networkteki cihazların haberleşmesi mümkün olmamaktaydı. Bu nedenle tüm cihazlar aynı üreticinin cihazı olmak durumundaydı. OSI referans modeli sayesinde bu dezavantaj ortadan kaldırılmıştır. OSI referans modeli 7 katmandan oluşmaktadır. Bu katmanlar aşağıda sunulmuştur.

1. Fiziksel Katman
2. Veri Bağlantı Katmanı
3. Ağ Katmanı
4. Taşıma Katmanı
5. Oturum Katmanı
6. Sunu Katmanı
7. Uygulama Katmanı

1.7.1.1 Fiziksel Katman

Fiziksel katman, verinin kablo üzerinde alacağı yapıyı tanımlar (İTÜ BİDB, 2013). Bu katmanda veriler bit olarak iletilir. Bu katman 1 ve 0'ların nasıl ışık, elektrik veya radyo sinyallerine çevrileceğini ve aktarılacağını tanımlar. Veri bu katmanda göndericide 1 ve 0'lar elektrik sinyaline dönüştürülüp kabloya yerleştirilir, karşı tarafta da bu elektrik sinyalleri okunur ve 0 ve 1'lere dönüştürülür. Verinin karşı tarafa, kullanılan fiber optik kablo, bakır kablo, radyo sinyalleri üzerinden nasıl gönderileceğini Fiziksel katman tanımlar. Veri akışının mümkün olabilmesi için iki tarafın aynı kurallar üzerinde tanımlanmış olması gerekir. Fiziksel katmanda bulunan cihazlara; kablo, fiber optik, hub ve tekrarlayıcı örnek verilebilir.

1.7.1.2 Veri Bağlantı Katmanı

Veri bağlantı katmanı fiziksel katman ile ağ katmanı arasında bağlantıyı sağlamaktadır. Fiziksel katmandan alınan bitleri ve ağ katmanında almış olduğu veri paketlerini framelere dönüştürür. Veri bağlantı katmanının büyük bir bölümü Ethernet kartı içinde gerçekleşir. Veri bağlantı katmanı ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin

tarafından kullanıldığıının tespiti ve fiziksel katmandan gelen verinin hatalara karşı kontrolü görevini yerine getirir (İTÜ BİDB, 2013). İkinci katman cihazlara modem, network kartı ve switch (anahtar) örnek verilebilir.

1.7.1.3 Ağ Katmanı

Verinin başka bir ağa iletilmesi durumunda yönlendiricinin kullanacağı bilgi ağ katmanında eklenir. Bağlantı katmanındaki çerçeveler bu katmanda paketler dönüştürülür. Ağ katmanında gönderen ile alıcı arasında en uygun yoldan verinin taşınması kontrol edilir. Bu katman sayesinde verinin yönlendiriciler (router) aracılığıyla yönlendirilmesi sağlanır. IP, IPsec, CLNS bu katmanda çalışır.

1.7.1.4 Taşıma Katmanı

Taşıma katmanı, verinin küçük paketlere bölünüp (karşı tarafın alabileceği kadar büyüklükte) gönderilmesinden sorumludur. Karşı taraftan gelen iletilmiş mesajından sonra sonraki paketin gönderilmesi işlemine geçilir. Bu katmanda veriler frameden segmente dönüşür. Bu katmanda çalışan protokollere TCP, UDP örnek verilebilir. Taşıma katmanı aynı zamanda verinin hatasız bir şekilde iletilmesinden de sorumludur. TCP bağlantısında veri çarpışmalardan dolayı karşı tarafa doğru iletilmemiş ise tekrar gönderilir. UDP bağlantıda ise tekrar gönderme işlemi yapılmaz (Anonim, 2012).

1.7.1.5 Oturum Katmanı

Oturum katmanında birden fazla cihaz ile iletişim halinde olunması durumunda gerekli ayarlamaları yapar. Oturum ile bağlantı arasındaki koordinasyonu sağlar. Bir cihazın en az iki bilgisayarlarla aynı anda haberleşmesi durumunda, doğru cihaz ile iletişimini sağlar. Sunuş katmanına yollanacak veriler farklı oturumlarla birbirinden ayrılarak yapılır. Bu katmandaki protokollere NetBIOS ve Sockets örnek verilebilir.

1.7.1.6 Sunuş Katmanı

Bu katmanın en önemli görevi yollanan verinin karşı cihaz tarafından anlaşılacak şekilde çevrilmesidir. Bu sayede farklı programların birbirlerinin verisini kullanabilmesi mümkün olur. Sunum katmanı, verinin kaynağında formatının belirlenmesi ve bunun karşı tarafta anlaşılmasından sorumludur. Veri bu katmanda şifreleme ve şifre çözmeler yapılır. Mov, JPEG vb. bu katmanda çalışır.

1.7.1.7 Uygulama Katmanı

Uygulama katmanı kullanıcılara en yakın olan katmandır. Kullanıcılar çeşitli yazılımlar sayesinde (web tarayıcısında işlem yapmak gibi) verilerini oluştururlar. OSI katmanlarında

sadece bu katman diğer katmanlara servis sağlamaz. Uygulamaların ağ üzerinde çalışması sağlanır. Bu katman kullanıcıların gereksinimini karşılar. DHCP, SSH, FTP, SNMP, HTTP, DNS protokolleri ve tarayıcılar bu katmanda çalışır.

1.8 Saldırı Tespit Sistemlerinde Kullanılan Veri Setleri

Saldırı Tespit Sistemleri, ağların güvenliğini sağlamada başat aktör konumundadır. Sistem sorumlularının IDS'e sahip olması ellerini güçlendirecek araçlardan bir tanesidir.

Araştırmacılar, saldırı tespiti konusunda bulmuş oldukları teknikleri test etme konusunda veri setlerine ihtiyaç duymaktadırlar. Araştırmacılar bazen kendi oluşturdukları veri setleri bazen de paylaşılmış olan veri setlerini kullanırlar.

Gelişen teknolojiye göre kötü yazılımlar da kendilerini güncellemektedir (Nehinbe, 2011). Bu doğrultuda veri setlerinin ortaya çıkan yeni saldırı türlerine göre güncellenmesi veri setinin başarısı açısından önem arz etmektedir.

Aşağıdaki Saldırı Tespit Sistemleri gelişiminde kullanılan 1998 ve 2016 yılları arasında paylaşılan veri setlerine ait genel bilgiler sunulmuştur.

1.8.1 DARPA (Lincoln Laboratuvarı – 1998/1999)

Ağ trafiğini analizi ve açıkları tespit etmek için oluşturulmuş veri setidir. Veri setinde e-mail, web site yükleme, FTP, SNMP, IRC ve Telnet trafiği bulunmaktadır. Şifre Tahmini, DoS, SynFlood, Rootkit, Buffer Taşması, FTP gibi saldırıları taşımaktadır. Bu veri seti o günün şartlarına göre iyi olmasına rağmen şu an yapılan saldırı türlerini içermediğinden eksiklik hissedilmektedir (McHugh, 2000).

1.8.2 KDD'99 (Massachusetts Teknoloji Enstitüsü– 1998/1999)

Tez çalışmamda kullandığım veri seti olması nedeni ile sonraki bölümde daha detaylı bir şekilde anlatılacaktır.

1.8.3 DEFCON (Shmoo Grup, 200/2002)

2000 yılında DEFCON-8 ve 2002 yılında DEFCON-10 şeklinde iki veri seti bulunmaktadır.

DEFCON-8 veri setinde port tarama ve arabellek taşma saldırıları bulunmaktadır.

DEFCOB-10 veri setinde ise Hedef port taraması, genel port taraması, FTP, Telnet, Yönetici Yetkisi ve Yanlış Paket saldırılarını barındırmaktadır (Sharafaldin ve ark., 2018). Bu veri setinde oluşturulurken gerçek bir network trafiği baz alınmadığından gerçekçi değildir. Bu veri seti uyarı korelasyon tekniklerini analizinde kullanılmıştır (Nehinbe, 2010).

1.8.4 CAIDA (Uygulamalı İnternet Veri Analiz Merkezi, 2002/2016)

CAIDA veri analiz merkezine ait 3 tane veri seti bulunmaktadır. Bunlar:

1.8.4.1 CAIDA OC48:

Bir servis sağlayıcısındaki trafiğin alınması ile elde edilmiş bir veri setidir. 2002 ve 2003 yıllarında bu veri seti oluşturulmuştur (Anonymous, 2002-2003). İnternet trafiğinin karakterize edilmesi, uygulama bozuklukları, güvenlik olayları, topolojik dağım ve akış hacmi-süresi ile ilgili araştırma yapan araştırmacıların başvurduğu bir veri setidir.

1.8.4.2 CAIDA DDoS

Bir saatlik DDoS saldırısına ait trafiğin 5 dakikalık kısmında oluşmaktadır.

1.8.4.3 CAIDA İnternet İzleri 2016

CAIDA'nın Equinix-Chicagoda bulunan yüksek hızdaki omurga switch üzerinde alınan trafik bilgisini içerir.

1.8.5 LBNL (Lawrence Berkeley National Laboratory Ve ICSI 2004-2005)

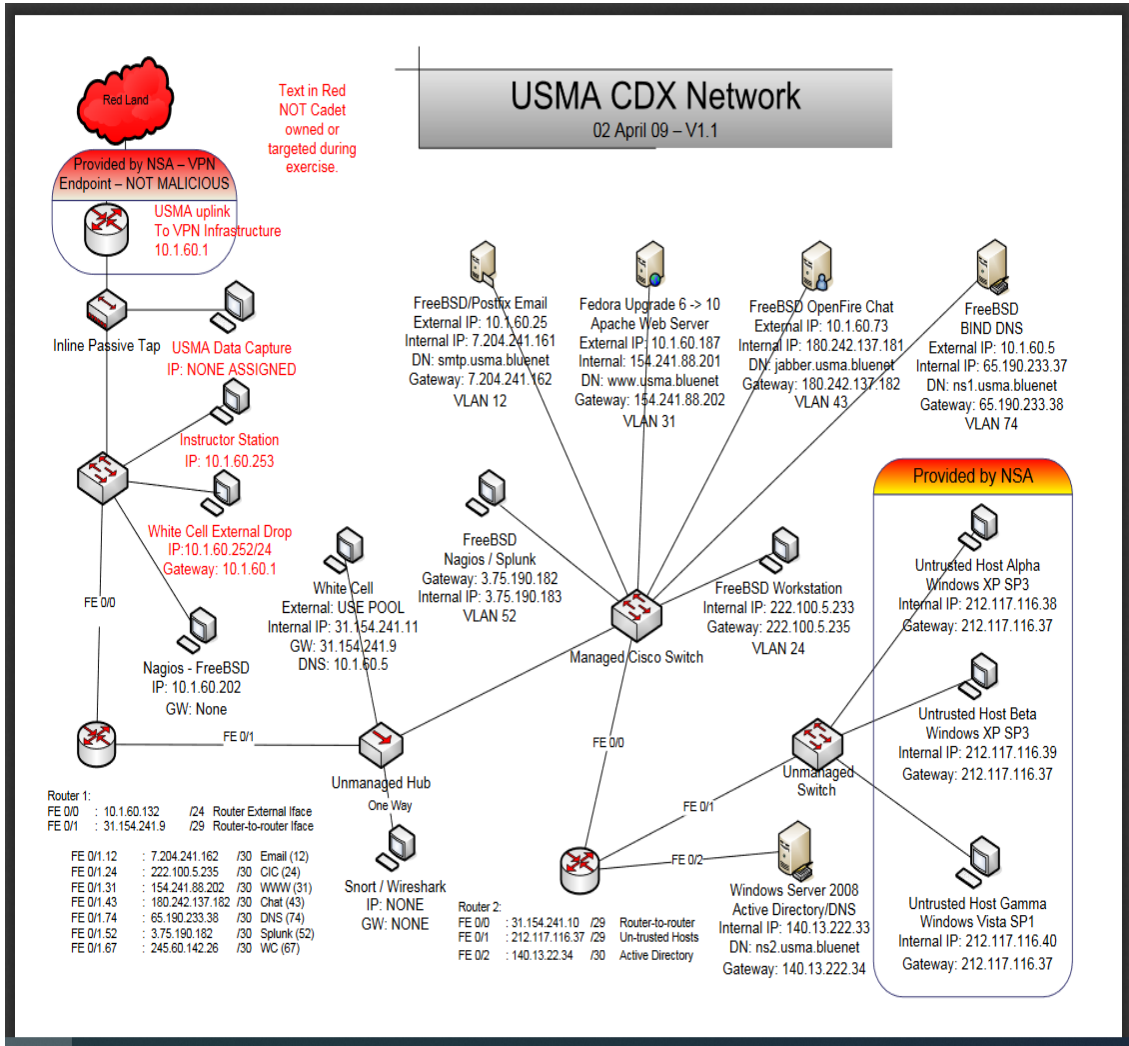
Orta büyüklükte bir sitenin trafiğinin analizi yapıp modern bir işletmeye benzerliğini ve farklı yönlerini ortaya koymak için yürütülen bir projedir (Nechaev ve ark., 2004).

Birden fazla sunucu içerisinde 100 saatlik veri toplanmıştır. Toplanan bu veriler kamu ile paylaşılmıştır. Bu veri seti sayesinde işletmelerdeki kalıpları ve dinamikleri kullanmaları için bir kaynak sağlanması umulmaktadır.

1.8.6 CDX (United States Military Academy 2009)

Web, elektronik posta, DNS gibi servislere ait trafiği barındırmaktadır.

Bu veri seti IDS test edilmesi açısından uygundur. Fakat veri setinin küçük olması ve çeşitliğinin az olması veri setinin eksiklikleri olarak sayılabilir (Sangster ve ark., 2009).



Şekil 1.1. Veri seti oluşturulurken kullanılan ağ yapısı (Anonymous, 2020).

1.8.7 Kyoto (Kyoto University 2009)

Bilgi sistemlerine izinsiz erişmek isteyenlere yönelik tuzak olarak kurulan sunuculara basküğü (Honeypots) denir. Bu veri seti honeypotlara yapılan saldırılarda elde edilmiş verilerden oluşmaktadır.

IDS, Kötü amaçlı yazılım tespiti ve NIDS analizinde kullanılabilecek on farklı özellik barındırmaktadır (Sharafaldin ve ark., 2018).

1.8.8 Twente (University of Twente 2009)

Bu veri seti, Kyoto Üniversitesindeki veri setinde olduğu gibi honeypotlarda elde edilmiştir. OpenSSH, Apache web sunucusu ve FTP servislerine yapılan 113 numaralı port üzerinde kimlik doğrulama yönelik yapılan trafiği barındırmaktadır.

Ayrıca veri seti içerisinde tamamen iyi veya kötü olmayan ICMP ve IRC trafiği de bulunmaktadır.

Veri setinin hacmi ve yapılan saldırı çeşitliği bakımında zayıf bir veri seti olarak kabul edilmektedir (Sperotto ve ark, 2009).

1.8.9 UMASS (University of Massachusetts 2011)

Massachusetts Üniversitesindeki kablosuz cihazların ve ağ paketlerinin izlem dosyalarında elde edilmiş veri setidir. TCP tabanlı indirme isteği saldırısına yönelik hazırlanmıştır.

Bu veri seti, saldırı çeşitinin az olması ve veri seti hacmi nedeni ile IDS ve IPS tekniklerinde kullanılması uygun değildir (Prusty ve ark., 2011).

1.8.10 ISCX2012 (University of New Brunswick 2012)

Bu veri setinde Alfa ve Beta şeklinde iki profil bulunmaktadır. Alfa profili çok aşamalı saldırı trafiğini barındırır. Beta profilinde ise gerçekçi bir ağ trafiğini bulundurmaz.

Veri setinde HTTP, SMTP, SSH, İMAP, POP3 ve FTP protokollerine ait trafik bulunur. Günümüz trafiğinin büyük bir kısmı https protokolünde olduğu bildiğinden ilgili protokole ait trafiğin olmaması ve simüle edilen saldırıların dağılım oranı gerçek dağılımdan farklı olması veri setinin eksi taraflarını oluşturmaktadır (Shiravi ve ark., 2012).

1.8.11 ADFA (University of New SouthWales 2013)

Bu veri setinde FTP ve SSH servislerine yönelik kaba kuvvet saldırıları, Java tabanlı meterpreter, sisteme yeni root kullanıcı ekleme, Linux meterpreter ve C100Webshel saldırılarını barındırır.

Saldırı çeşitliliği ve normal ile saldırı davranışları iyi ayırt edilmemesi bu veri setinin eksiklikleridir (Hu ve ark., 2014).

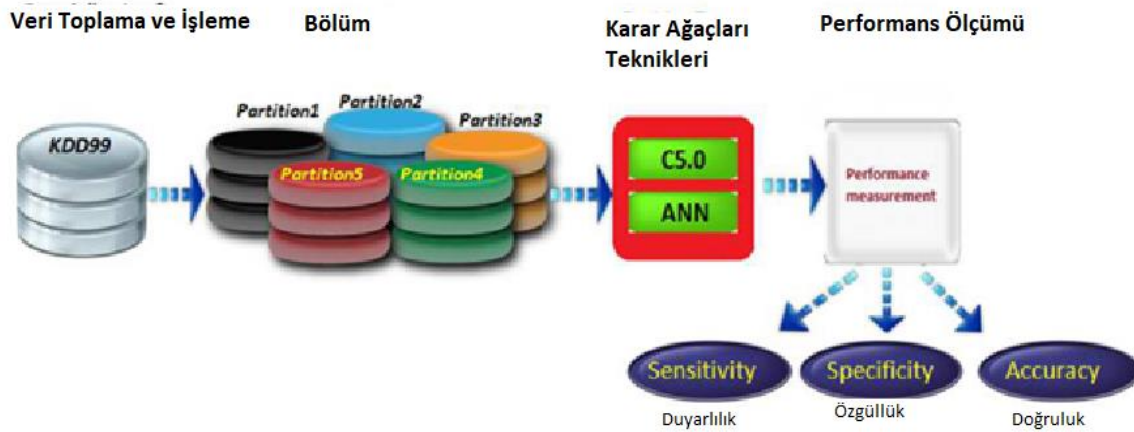
2. KAYNAK ARAŞTIRMASI

Saldırı tespit sistemlerinde klasik yöntemlerin (imza tabanlı STS) artık yeteri kadar güvenli olmadığına anlaşılmaya başlandı ve üzerine yeni modeller ortaya çıkmıştır.

H. Tanrıku ve ark. (2009), Darpa tarafından bir kamu ağındaki trafiğin analizi ile elde edilmiş veri setini kullanarak, Çok Katmanlı Algılayıcılar (Multi Layer Perceptron) modeli kullanarak bir ağda yapılacak DoS saldırılarını tespit etmişlerdir.

Heba F. Eid ve ark., (2010), KDD'99 veri seti üzerinde, Temel Bileşen Analizi (Principal Component Analysis- PCA) ile Destek Vektör Makineleri (Support Vector Machines- SVMs) kullanarak oluşturulacak modelin karmaşıklığını azaltmak için bazı parametrelerde eksilmeye gitmiştir. Yapılan testlerle özellik seçimi ile optimum modeli ortaya koymuşlardır.

Pratibha Soni ve ark., (2014), modelin öğrenmesi için KDD'99 veri setinin %10'luk dilimi kullanmıştır. "An Intrusion Detection System Based on KDD-99 Data using Data Mining Techniques and Feature Selection" adlı çalışmalarında C5.0 Karar Ağaçları ve Yapay Sinir Ağları kullanılarak belli özellikler üzerinde doğruluk oranlarını ortaya konulmuştur. Yapılan çalışmada eğitim ve test veri setlerindeki oranların modelin doğruluk üzerindeki etkisi de belirtilmiştir.

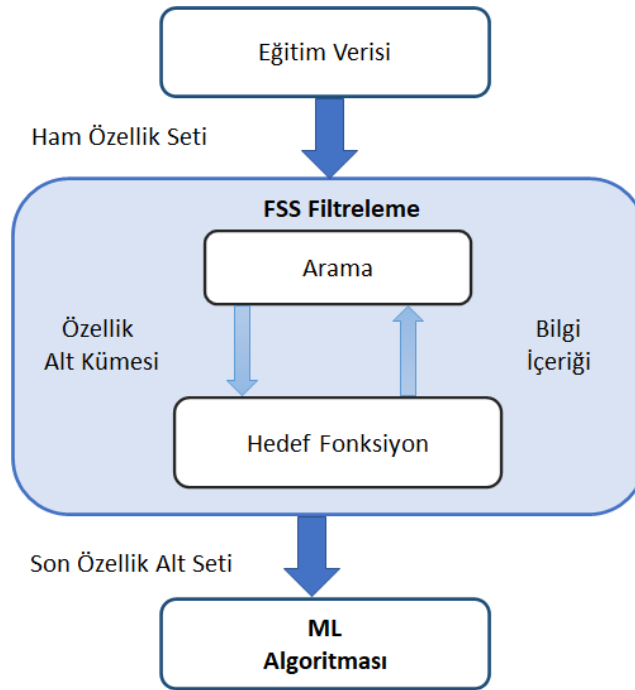


Şekil 2.1. C5.0 ve YSA Tekniğini Kullanarak Model Geliştirme ve Test Etme Süreci (Pratibha Soni ve ark., 2014).

Juan Hu (2014), yanlış alarm oranlarını düşürürken algılama oranlarını artırma çabası içinde, ayrık sistem çağrı modellerini kullanan yeni bir host tabanlı anomali saldırı tespit

metodolojisini ortaya koymuştur. Modelin oluşturulmasında KDD98 ve UNM veri setleri kullanılmıştır. Bu çalışmada, güncel hackleme yöntemi ve mevcut işletim sistemleri kullanılarak ADFA Linux veri seti oluşturulmuştur.

Harbora ve ark. (2014), KDD'99 veri setinin %10 luk dilimini veri madenciliği algoritmalarını test etmek için kullanmışlardır. Veri ilişkilendirme kuralları, ön işleme, regresyon, sınıflandırma, kümeleme ve ilişkilendirme kuralları ile görselleştirme için algoritma ve araçlarını barındıran WEKA kullanılmıştır. Bununla birlikte, algoritmanın performansını ölçmek için karışıklık matrisi kullanılmıştır. Çalışmada, 64 bit Windows 8 işletim sistemi, 4 GB Ram, Intel i5 2.6 GHz işlemciye sahip bir bilgisayar üzerinde WEKA aracı kullanılarak testler yapılmıştır. SVM, ANN, KNN, Nave-Bayes ve Decision Tree algoritmaları kullanılmıştır. Bu algoritmalarından en başarılı sonuç 0,997 ile KNN'de elde edilmiştir.



Şekil 2.2. JAVA-ML Kütüphanesi ile özellik seçimi (Harbora ve ark., 2014)

Giftty Jeya ve ark. (2012) yaptıkları çalışma FLDA ile yöntemi ile User to Root ve Remote to Local saldırılarını tespit etmek için model geliştirmişlerdir. Modelin öğrenmesinde KDD'99 veri seti kullanılmıştır. KDD'99 veri kümesinde bulunan özelliklerin bazılarında eksilmeye gidilmiştir. Özellik seçimi için SPSS programı kullanılmıştır. Modelin başarısı U2L için %99,9 iken R2L için bu oran ancak %73,2'dir.

Obeida ve ark. (2019), KDD'99 veri seti üzerinde farklı sınıflandırma algoritmalarıyla modelin doğruluk seviyesini ölçmüşlerdir. Testler Ubuntu versiyon 13.10 işletim sistemi kurulu workstation üzerinde yapılmıştır. Cihaz, Intel Xeon (R) CPU E5-2680 @ 2.70GHzX4 ve 8 GB RAM'e sahiptir. Yazılım olarak Weka sürüm 3.7.12 kullanılmıştır. Test için eğitim veri setinden bağımsız 60.000 adet örneklem alınmıştır. Çalışmada; J48, Random forest, Random Tree, Decision Table, Multilayer Perceptron (MLP), Naïve Bayes ve Bayes Network sınıflandırma algoritmaları kullanılmıştır.

Tablo 2.1. Doğruluk oranı (Obeida ve ark.,2019)

Sınıflandırıcı	Doğru Sınıflandırılmış Örnek	Yanlış Sınıflandırılmış Örnek	Doğruluk
J48	55865	4135	93,108%
Random Forest	56265	3735	93,775%
Random Tree	54343	5655	90,575%
MLP	55141	4859	91,901%
Naive Bayes	54741	5259	91,235%
Bayes Network	54439	5561	90,731%

3. MATERYAL VE YÖNTEM

3.1 Materyal

Bu çalışmada, MIT Lincoln Laboratuvarında 9 haftalık süreçte elde edilmiş verilerin 1999 yılında güncellenmiş hali olan KDD'99 veri seti materyal olarak kullanıldı. Veri setinde var olan verilerden yola çıkılarak yeni değerler eklendiştir (Üst sınıf verisi: DoS, User to Root, Remote to Local ve Probe, vb.).

KDD'99 veri setinde olan ancak SPSS veri analiz programında yapılan analizler neticesinde sonuç üzerinde etkisi olmayan ya da az olduğu tespit edilen; flag, su_attempted, num_file_creations, num_shells, num_access_files ve is_host_login parametreleri modele dâhil edilmeden sonuçlar ortaya konulmuştur.

Veri analiz programı olarak IBM SPSS 22 sürümü kullanılmıştır. Programlama dili olarak ise dördüncü nesil bir programlama dili ve sayısal hesaplama yazılımı olan Matlab kullanılmıştır.

Test süreci, Intel® Xeon® Gold 6140 @ 2.30 GHz işlemci ve 32 GB RAM'e sahip Windows 10 Pro 64 Bit işletim sistemine sahip bilgisayarda yapılmıştır.

3.1.1 KDD'99

1998 yılında DARPA Saldırı Tespit Değerlendirme programı kapsamında MIT Lincoln Laboratuvarında elde edilmiş verilerin güncellenmiş halidir (Sharafaldin ve ark., 2018).

Veri setinde, Lincoln Laboratuvarında Amerika Birleşik Devletler Hava Kuvvetlerine ait yerel bir ağın oluşturulan örneğinden 9 hafta boyunca elde edilen bağlantılar ile birlikte yapılan birden fazla saldırıya ait veriler bulunmaktadır (Salvatore ve ark., 1999).

KDD'99 saldırı tespit sistemleri için model dizayn etmede kullanılan geniş bir veri setidir (Sharafaldin ve ark., 2018). Bu veri seti 41 adet giriş ve 1 adet çıkış olmak üzere 42 parametre ve 4.940.200 adet bağlantıdan oluşmaktadır.

a. **Giriş parametreleri**

1. TCP bağlantısının temel özellikleri.
2. Bağlantıya ait içerik özellikleri.
3. İki saniyelik zaman içerisinde elde edilen trafik özellikleri.
4. İki saniyeden uzun saldırılarda ana bilgisayar özellikleri.

Tablo 3.1. TCP bağlantısının temel özellikleri

Özellik Adı	Açıklaması
duration	Bağlantı süresi (saniye cinsinde)
protocol_type	Bağlantının protokol tipi: tcp, icmp, v.b.
service	Kullanılan servis: http, ftp, v.b.
src_bytes	Kaynaktan hedefe gönderilen verinin byte sayısı
dst_bytes	Hedeften kaynağa gönderilen verinin byte sayısı
flag	Bağlantının normal ya da hatalı durumu
land	1: Bağlantı aynı hosta/hostta. 0: Diğer durumlar için
wrong_fragment	Yanlış parçalama sayısı
urgent	Acil paket sayısı

Tablo 3.2. Bağlantıya ait içerik özellikleri

Özellik Adı	Açıklaması
hot	“hot” gösterge sayısı
num_failed_logins	Başarısız giriş deneme sayısı
logged_in	1: Giriş başarılı, 0: Diğer durumlar
num_compromised	“compromised” kuşullarının sayısı
root_shell	1: Root hakları elde edildi. 0: Diğer durumlar
su_attempted	1: “su root” komutu denenmiştir. 0: Diğer durumlar
num_root	“root” erişim sayısı
num_file_creations	Dosya oluşturma işlemlerinin sayısı
num_shells	Shell prompts sayısı
num_access_files	Number of operations on access control files
num_outbound_cmds	Bir ftp oturumundaki giden komutların sayısı
is_hot_login	1: Giriş “hot” listesine aitse. 0: Diğer durumlar
is_guest_login	1: Giriş misafir girişidir. 0: Diğer durumlar

Tablo 3.3. İki saniyelik zaman içerisinde elde edilen trafik özellikleri

Özellik Adı	Açıklaması
count	Son iki saniyedeki mevcut bağlantıyla aynı ana bilgisayara bağlantı sayısı
serror_rate	“SYN” hataları olan bağlantıların yüzdesi
rerror_rate	“REJ” hataları olan bağlantıların yüzdesi
same_srv_rate	Aynı hizmete bağlantı yüzdesi
diff_srv_rate	Farklı hizmete bağlantı yüzdesi
srv_count	Son iki saniye içinde geçerli bağlantıyla aynı hizmete bağlantı sayısı
srv_serror_rate	“SYN “ hataları olan bağlantıların yüzdesi
srv_rerror_rate	“REJ “ hataları olan bağlantıların yüzdesi
srv_diff_host_rate	Farklı ana bilgisayarlara bağlantı yüzdesi

Tablo 3.4. İki saniyeden uzun saldırılarda ana bilgisayar özellikleri

Özellik Adı	Açıklaması
dst_host_count	Aynı hedef IP adresine yapılan bağlantıların toplamı
dst_host_srv_count	Aynı hedef port numarasına yapılan bağlantıların toplamı
dst_host_same_srv_rate	“dst_host_count” içinde toplanan bağlantılar arasında aynı hizmete giden bağlantıların yüzdesi
dst_host_diff_srv_rate	dst_host_count içinde toplanan bağlantılar arasında farklı hizmetlere olan bağlantıların yüzdesi
dst_host_same_src_port_rate	dst_host_srv_count içinde toplanan bağlantılar arasında aynı kaynak bağlantı noktasına giden bağlantıların yüzdesi
dst_host_srv_diff_host_rate	dst_host_srv_count içinde toplanan bağlantılar arasında farklı hedef makinelere giden bağlantıların yüzdesi

Özellik Adı	Açıklaması
dst_host_serror_rate	dst_host_count içinde toplanan bağlantılar arasında “SYN” bayrağını etkinleştiren bağlantıların yüzdesi
dst_host_srv_serror_rate	dst_host_srv_count içinde toplanan bağlantılar arasında “SYN” bayrağını etkinleştiren bağlantıların yüzdesi
dst_host_rerror_rate	dst_host_count içinde toplanan bağlantılar arasında REJ işaretini etkinleştiren bağlantıların yüzdesi
dst_host_srv_rerror_rate	dst_host_srv_count içinde toplanan bağlantılar arasında REJ işaretini (4) etkinleştiren bağlantıların yüzdesi

Veri setinde bulunan saldırılar 4 ana kategoride tanımlanabilir. Bunlar:

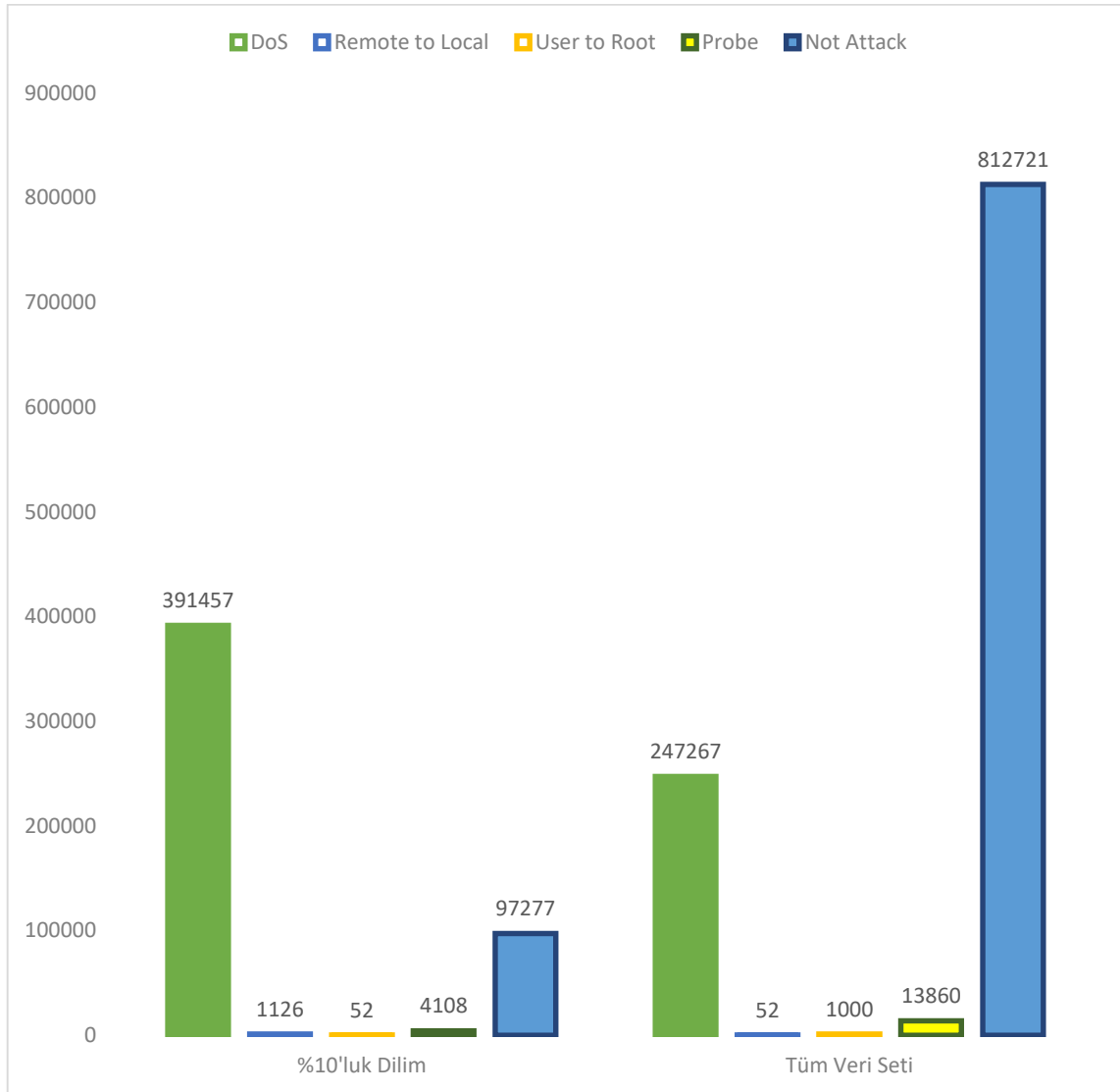
1. DOS: denial-of-service, Ağda bulunan bir cihazın sistem kaynaklarını tüketerek gerçek kullanıcılara hizmet veremeyecek duruma getirmedir. Örnek saldırı syn flood.
2. R2L(Remote to Local): Bir sisteme erişim izni olmadan bağlanmaya çalışma. Örnek saldırı guessing password.
3. U2R (User to Root): Normal kullanıcı hakkına sahipken admin ya da root kullanıcı haklarını elde etme saldırı türüdür. Örnek buffer overflow.
4. Probing: Bu saldırıda hedef cihaz hakkında bilgi toplama yapılır. Bu bilgi açık olan portlar, geçerli ip adresleri, üzerinde çalışan servisler, kurulu olan işletim sistemi vb. Örnek port scanning.

Tablo 3.5. KDD veri setindeki kategorize edilmiş ataklar.

Saldırı Kategorisi	Saldırı Tipi
DoS (Denial of Service)	back, land, neptune, pod, smurf, teardrop
R2L (Remote to Local)	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster
U2R (User to Root)	buffer_overflow, loadmodule, perl, rootkit
Probe	ipsweep, nmap, portsweep, satan

Tablo 3.6. KDD veri setindeki saldırıların numerik karşılığı ve eklenen Üst sınıf Verisi.

Saldırı Adı	Saldırı Numerik	Üst Sınıf Değer
back	0	0
buffer_overflow	1	2
ftp_write	2	1
guess_password	3	1
imap.	4	1
ipsweep	5	3
land.	6	0
loadmod	7	2
multiho	8	1
neptune	9	0
nmap.	10	3
normal.	11	4
perl.	12	2
phf.	13	1
pod.	14	0
portswe	15	3
rootkit	16	2
satan	17	3
smurf.	18	0
spy	19	1
teardrop	20	0
warezclient	21	1
warezmaster	22	1



Şekil 3.2. Üst Sınıflara göre kategorize edilmiş saldırı istatistikleri

Tablo 3.7. KDD'99 Veri setinin %10'luk dilimindeki saldırılar ve yüzdelikleri.

Sıra	Saldırı Çeşidi	Adet	Yüzdelik
1	buffer_overflow	30	0,0
2	Back	2203	0,4
3	ftp_write	8	0,0
4	guess_passwd	53	0,0
5	İmap	12	0,0

Sıra	Saldırı Çeşidi	Adet	Yüzdelik
6	İpsweep	1247	0,3
7	Land	21	0,0
8	Loadmodule	9	0,0
9	Multihop	7	0,0
10	Neptune	107201	21,7
11	Nmap	231	0,0
12	Normal Paket	97277	19,7
13	Perl	3	0,0
14	Phf	4	0,0
15	Pod	264	0,1
16	Portsweep	1040	0,2
17	Rootkit	10	0,0
18	Satan	1589	0,3
19	Smurf	280789	56,8
20	Spy	2	0,0
21	Teardrop	979	0,2
22	Warezclient	1020	0,2
23	Warezmaster	20	0,0
	Toplam	494020	100,0

Tablo 3.8. KDD'99 Veri seti tekrarlı verinin elenmesi sonrası saldırılar ve yüzdeleri

Sıra	Saldırı Çeşidi	Adet	Yüzdelik
1	buffer_overflow	968	0,1
2	Back	30	0,0
3	ftp_write	8	0,0
4	guess_passwd	53	0,0
5	İmap	12	0,0
6	İpsweep	3723	0,3
7	Land	19	0,0
8	Loadmodule	9	0,0
9	Multihop	7	0,0
10	Neptune	242149	22,5
11	Nmap	1554	0,1
12	Normal Paket	812721	75,6
13	Perl	3	0,0
14	Phf	4	0,0
15	Pod	206	0,0
16	Portsweep	3564	0,3
17	Rootkit	10	0,0
18	Satan	5019	0,5
19	Smurf	3007	0,3
20	Spy	2	0,0
21	Teardrop	918	0,1
22	Warezclient	893	0,1
23	warezmaster	20	0,0
	Toplam	1074900	100,0

3.1.1.1. Saldırı Tipleri

3.1.1.1.1. Buffer_overflow (U2R)

Sınırlandırılmış bellek alanına kapasitesinin üzerinde veri yazma işlemidir. Örnek olarak 10 karakter olarak tanımlanan bir değişkene, 11 karakterlik değer ataması yapılırsa

bunda 1 karakterlik bellek taşması meydana gelecektir. Saldırganlar bu açığı tespit ettiğinde taşan kısma kendi kodlarını yazar ve sistemi kendi amaçları doğrultusunda kullanır.

3.1.1.1.2. Back (DoS)

Apache web sunucularında URL içerisinde backslash gönderilerek yapılan hizmet durdurma saldırısıdır.

3.1.1.1.3. FTP Write(R2L) Saldırısı

Bu saldırıda, yanlış yapılandırılmış olan bir FTP sunucusuna saldırganın yetkisi olmadan dosya yazmasıdır. Saldırgan, FTP sunucusuna yazmış olduğu dosya ile erişim sağlamış olur.

3.1.1.1.4. Guess_Passwd Saldırısı (R2L)

Hedef sisteme giriş yapmak için kullanılan şifreyi deneme yanılma yöntemi kullanılarak elde etmeye çalışmaktır. Bu saldırı kaba kuvvet saldırısı olarak da tanımlanır.

3.1.1.1.5. IMAP(R2L) Saldırısı

Bu saldırı, hedef sisteme IMAP doğrulama metodu ile kullanıcı adı ve şifre denemeleri yaparak sisteme girmeye çalışmadır.

3.1.1.1.6. IPSweep (Probe) Saldırısı

Saldırgan hedef sistemin up ya da down olduğu bilgisi için hedefe ping isteği gönderir. Hedef, ping isteğine cevap verirse hedefin canlı olduğunu anlar.

3.1.1.1.7. LAND (Local Area Network Denial) (Dos) Saldırısı

Bu saldırı katman 4 saldırısıdır. Saldırgan, kaynak ve hedef IP adresi ve portu aynı olan sahte bir TCP SYN yollar. Hedef makine bu isteğe cevap vermeye çalıştığında bir döngüye girer ve hizmet veremez duruma gelir.

3.1.1.1.8. Loadmodule (U2R) Saldırısı

Loadmodule, Window System Sunuclarında dinamik olarak yüklenebilen iki çekirdek sürücüsünü o anda çalışan sisteme yükler ve bu modülleri kullanmak için dizinde özel aygıtlar oluşturmak için kullanır. Loadmodule programının ortamını sterilize etme şeklindeki bir hata nedeniyle, yetkisiz kullanıcılar yerel makineye kök erişimi sağlamasıdır.

3.1.1.1.9. Multihop (R2L)

Kullanıcının ilk önce bir makineye girdiği çok günlük senaryodur. Multihop saldırısı bazen yetki yükseltmesi bazen dışardan yapılan saldırı olabilmektedir. KDD'99 veri setinde ise Remote to Local saldırısı olarak yapılmıştır.

3.1.1.1.10. Neptune (SYN Flood) (DOS) saldırısı

Bir TCP bağlantısı başlamadan önce üçlü el sıkışma işlemi yapılır. Öncelikle istemci sunucuya SYN bayrağını aktif halde gönderir. İkinci işlem olarak da sunucu SYN ve ACK bayraklarını bir olarak geri gönderir. Son işlemde ise İstemci ACK bayrağını aktif olarak gönderir. Bu işlemlerden sonra bağlantı sağlanmış olur. Saldırgan hedef makineye kaynağı aktif olarak kullanılmayan kaynaklardan geliyormuş gibi paketler gönderir. Sunucu gönderilen her pakete SYN ACK bayrağı aktif bir şekilde cevap gönderip bu işleme kaynak ayırır. Bir süre sonra sunucunun kaynağı dolar ve gerçek bir bağlantı paketi gelse bile sunucu bağlantı sağlamaz.

3.1.1.1.11. NMAP (Probe) Saldırısı

Hedef sistem hakkında bilgi toplama amacıyla yapılan işlemdir. Nmap ile hedef cihazın açık portları, kullanmış olduğu işletim sistemi, çalışan fiziksel aygıtlar, firewalla sahip olup olmadığı ve ağ kartı üreticisi, çalışan servisler gibi bilgiler alınabilir. Alınan bu bilgiler doğrultusunda saldırı hedef sisteme sızmaya çalışır.

3.1.1.1.12. Perl

Perl dilinde yazılmış, normal kullanıcı yetkisine sahipken root ya da admin yetkisine yükseltme saldırısıdır.

3.1.1.1.13. Phf

Bu saldırı, Web sunucusunda yanlış yapılandırma neticesinde istemciler tarafından CGI kod bloğu çalıştırabilme ve kendi amaçları doğrultusunda hareket ettirme.

3.1.1.1.14. PoD

Hedef cihaza, alabileceğinden daha büyük ping paketi göndererek cihazın donmasına ya da çökmesine neden olan saldırı tipidir. Bazı sistemler maksimum Ping değerinden daha büyük paketleri işleyemez bu durumda sistemin çökmesine ya da donmasına neden olur. Buna karşı önlemler alındığında şuan için çok yapılan bir saldırı değildir.

3.1.1.1.15. Portsweep (Probe)

Hedef cihaz ya da cihazlarda belirtilen port özelinde sorgulama yapılır. Bu noktada PortScan saldırısından farklı olmaktadır. PortScan saldırısında hedef sistem ya da sistemlere belli bir port numara aralığı ile sorgulama yapılır açık bulunan port üzerinden o portun zafiyetinden yararlanarak saldırı gerçekleştirilir.

3.1.1.1.16. Rootkit (U2R)

Rootkit veya root kit terimi, başlangıçta "root" erişimi veren Unix benzeri bir işletim sistemi için kötü amaçla değiştirilmiş bir dizi yönetimsel araçları ifade eder. Bir davetsiz misafir bir sistemdeki standart yönetim araçlarını bir rootkit ile değiştirebiliyorsa, davetsiz misafir sistem üzerinde kök erişim elde eder ve bunu sistem yöneticisinden gizleyebilir.

3.1.1.1.17. Satan (Probe)

Hedef sistemlere yönelik ağda bilgi toplamak için yapılan saldırıdır. Sistem yöneticileri bunu ağın analizi için kullanırken saldırganlar ise hedef sistem ya da networkun açığını tespit edip ortan içeriye girmeye çalışmaktadır.

3.1.1.1.18. Smurf (DOS) saldırısı

Bu saldırı türünde saldırgan networkteki hostlara ICMP paketi gönderir. Fakat gönderen kısım olarak hedef makinanın IP adresi belirtilir. Dolayısı ile hedef makina ağıdaki tüm cihazlar tarafından ICMP cevap paketi döner. Bir süre sonra hedef makine bu cevap paketlerini alamayacak duruma gelir ve düşer.

3.1.1.1.19. Spy (R2L)

Çeşitli yöntemlerle hedef sistemden bilgi elde etme için yapılan çok günlü senaryo yapılan saldırıdır.

3.1.1.1.20. Teardrop (Dos)

Bu saldırı türünde saldırgan, kurban makinasına özel hazırlanmış paket gönderir. TCP/IP Protokolünde gönderilen paketler karşı tarafın MTU değerinden büyük ise paketler daha küçük parçalara bölünür ve o şekilde gönderilir. Bu işleme parçalama (Fragmentation) denir. Paketler karşı tarafa gönderildikten sonra birleştirme işlemi yapılır. Parçalanmış paketler gönderilirken offset değeri de gönderir. Karşı tarafta parçalanmış paketlerin birleştirilmesi offset değerine göre yapılır. Saldırgan offset değerlerinin çakışmasını sağlar ve karşı tarafta da bu duruma karşı bir önlem alınmamışsa makine cevap veremeyecek duruma gelir.

3.1.1.1.21. Warezclient

Bu saldırı Warezmaster saldırısının devamı niteliğindedir. FTP sunucularının yanlış yapılandırması neticesinde ortaya çıkan bir Remote to Local saldırısıdır. FTP sunucuları kullanıcı adı ve şifre girişi yapılmadan bağlanabilme yöntemini destekler. Bazı durumlarda sistem sorumluları tarafından yanlış konfigürasyon neticesinde anonim kullanıcılarda, normalde yazma yetkisi olmaması gerekirken yazma yetkisi verilmektedir. Saldırgan bunu

tespit etmesi durumunda sunucuya kendi dosyalarını yükler ve FTP sunucusuna bağlanan diğer kullanıcıların bu dosyaları indirmesini sağlar.

3.1.1.1.22. Warezmaster

FTP sunucularının yanlış yapılandırması neticesinde ortaya çıkan bir Remote to Local saldırısıdır. FTP sunucuları kullanıcı adı ve şifre girişi yapılmadan bağlanabilme yöntemini destekler. Bazı durumlarda sistem sorumluları tarafından yanlış yapılandırma neticesinde anonim kullanıcılarda, normalde yazma yetkisi olmaması gerekirken yazma yetkisi verilmektedir. Saldırgan bunu tespit etmesi durumunda sunucuya kendi dosyalarını yükler. FTP sunucusuna usulsüz dosya (Warez) atması Warezmaster saldırısı olarak tanımlanır.

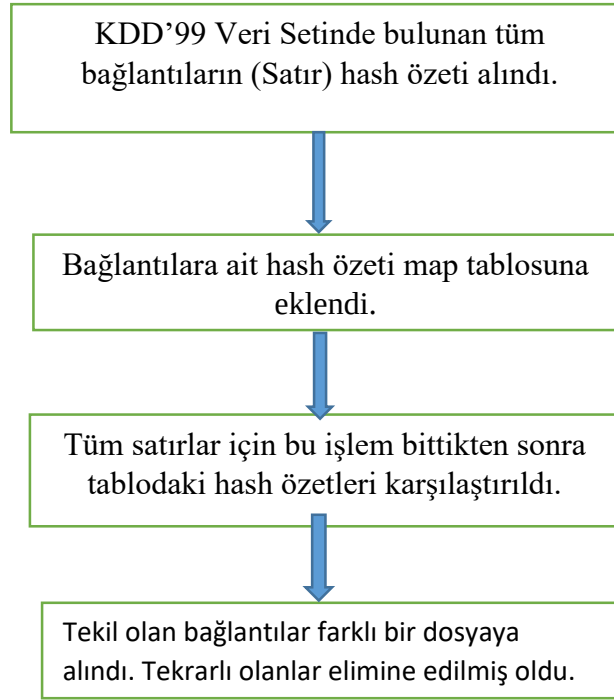
3.1.1.2. Eliminasyon İşlemi

KDD'99 anomali tabanlı saldırı tespit sistemleri dizaynında en çok kullanılan veri setidir. Veri seti içinde çok fazla tekrarlı bağlantı mevcuttur. Toplam bağlantı âdeti 4.940.200 iken tekrarlı verinin eliminasyonu sonrası 1.074.900 (3.865.300 adet tekrarlı bağlantı bulunmaktadır) veriye düşmektedir. Bu da yaklaşık olarak %78 oranında tekrarlı verinin olduğu anlamına gelmektedir. KDD'99 veri seti %10 luk dilimdeki saldırı istatistikleri tüm veri setindeki saldırı istatistikleri ile uyuşmamaktadır. KDD'99 veri seti içerisinde; 6 Adet DoS, 8 Adet Remote to Local, 4 Adet User to Root ve 4 adet de Probe saldırısı olmak üzere toplam 22 Adet saldırı tipi bulunmaktadır.

KDD'99 veri seti, MIT Lincoln Laboratuvarında 9 haftalık süreçte elde edilmiş verilerin 1999 yılında güncellenmiş halidir. KDD'99 veri setindeki bazı saldırılar güncelliğini yitirmiştir.

Ağ güvenliği her geçen gün daha önemli bir hal almaktadır. Siber güvenliğe ayrılan bütçe de bu doğrultuda artmaktadır. Ağ güvenliğini sağlamadaki bileşenlerinden “saldırı tespit sistemleri” için oluşturulmuş olan KDD'99 veri seti, akıllı model tasarlamaya büyük katkı sağlamaktadır.

KDD'99 veri setinde bulunan tekrarlı verinin eleme işlemi java ile yazılan kod ile yapılmıştır. Her bir satırın şifrelenmiş hali alındı ve aynı şifre yapısına sahip satırlar elenerek elde edildi. Elimine işlemi aşağıda gösterildiği gibidir,



Şekil 3.3 Tekrarlı verinin eleme işlemi.

3.1.1.3. KDD Veri Setine Eklenen Çıkış Değişkenleri

Veri setinde bulunan özelliklere ek olarak öncelikle yapılan saldırılar sınıflandırma işlemine tabi tutuldu. Bu sınıflandırma işlemi aşağıdaki gibi yapılmıştır.

- a. DoS – (back, land, neptune, pod, smurf, teardrop)
- b. R2L (Remote to Local) (ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster)
- c. U2R (User to Root) (buffer_overflow, loadmodule, perl, rootkit)
- d. Probe (ipsweep, nmap, portsweep, satan)

Daha sonra olaya daha genel bakabilmek adına yapılan trafik, saldırı ya da normal paket şeklinde sınıflandırıldı.

3.1.1.4. Bağımsız Değişkenlerin Sonuç Üzerindeki Etkileri

KDD'99 veri setinde 41 adet bağımsız değişken mevcuttur. Bu değişkenlerin sonuç üzerindeki etkisi için istatistik programından (IBM SPSS) faydalanmıştır.

İkiden fazla değişkenin birebirleri ile olan ilişkilerini ölçmek için kullanılan yöntem Regresyon Analizi yöntemidir. Regresyon analizi yöntemi ile değişkenlerin arasında ilişki olup olmadığı ve olması durumunda bunun şiddeti ortaya konulur.

Bağımsız değişkelerle sonuç üzerindeki etkisini belirlemek için regresyon işlemine tabi tutulmuştur.

Tablo 3.9. Bağımsız değişkenin bağımlı değişken üzerindeki etkisi.

Model		Standartlanmamış Katsayılar		Standartlanmış Katsayılar	t	Sig.
		B	Std. Error	Beta		
	(Sabit)	8,137	,030		269,080	0,000
	Duration	4,485E-6	,000	,005	7,008	0,000
	Protocol_Type	-0,211	,004	-,050	-54,377	0,000
	service	-0,001	,000	-,007	-7,731	0,000
	flag	0,006	,004	,011	1,522	0,128
	src_bytes	4,099E-9	,000	,007	11,417	0,000
	dst_bytes	3,192E-9	0,000	0,004	6,099	0,000
	land	-0,662	0,147	-0,003	-4,501	0,000
	wrong_fragment	3,001	0,008	0,217	360,847	0,000
	urgent	-0,154	0,048	-0,002	-3,219	0,001
	hot	0,059	0,001	0,048	48,266	0,000
	num_failed_logins	-1,557	0,046	-0,020	-33,504	0,000
	logged_in	0,099	0,004	0,039	22,877	0,000
	num_compromised	-0,026	0,001	-0,175	-17,875	0,000
	root_shell	-0,704	0,047	-0,010	-15,029	0,000
	su_attempted	0,117	0,055	0,002	2,127	0,033
	num_root	0,026	0,001	0,176	17,796	0,000
	num_file_creations	-0,003	0,003	-0,001	-1,207	0,227
	num_shells	-0,083	0,039	-0,001	-2,136	0,033
	num_access_files	0,011	0,010	0,001	1,030	0,303
	is_host_login	-1,389	0,528	-0,002	-2,631	0,009
	is_guest_login	-0,107	0,020	-0,005	-5,370	0,000

Model	Standartlanmamış Katsayılar		Standartlanmış Katsayılar	t	Sig.
	B	Std. Error	Beta		
count	0,004	0,000	0,258	182,584	0,000
srv_count	0,005	0,000	0,122	153,089	0,000
serror_rate	-0,702	0,035	-0,225	-19,891	0,000
srv_serror_rate	0,511	0,037	0,164	13,948	0,000
rerror_rate	1,280	0,031	0,280	41,335	0,000
srv_rerror_rate	-1,054	0,024	-0,229	-44,530	0,000
same_srv_rate	3,010	0,008	0,965	385,658	0,000
diff_srv_rate	2,970	0,008	0,284	362,520	0,000
srv_diff_host_rate	-0,076	0,003	-0,017	-26,111	0,000
dst_host_count	-0,001	0,000	-0,059	-72,190	0,000
dst_host_srv_count	0,001	0,000	0,098	54,368	0,000
dst_host_same_srv_rate	-0,264	0,006	-0,092	-42,640	0,000
dst_host_diff_srv_rate	1,176	0,009	0,126	126,904	0,000
dst_host_same_src_port_rate	0,222	0,004	0,042	51,248	0,000
dst_host_srv_diff_host_rate	-4,464	0,017	-0,206	-265,754	0,000
dst_host_serror_rate	-0,409	0,025	-0,131	-16,570	0,000
dst_host_srv_serror_rate	0,623	0,031	0,200	20,057	0,000
dst_host_rerror_rate	-0,234	0,013	-0,050	-18,624	0,000
dst_host_srv_rerror_rate	0,599	0,012	0,128	49,754	0,000
Bağımlı Değişken: Saldırı					

Bağımsız değişkenlerin bağımlı değişken üzerindeki etkisine bakmak için yukardaki tabloda sigmoid değerine bakmak gerekmektedir. **sigmoid < 0,008** olması durumunda bağımsız değişken değişken üzerinde etkilidir denilebilir.

KDD'99 veri seti özelinde baktığımızda flag, su_attempted, num_file_creations, num_shells, num_access_files ve is_host_login değişkenlerinin bağımlı değişken üzerindeki etkisinin düşük olduğu görülecektir.

Bu nedenle modelleme yapıldığında yukarda sayılan özelliklerin bulunduğu ve elemine edildiği durumlar ayrı ayrı uygulanacaktır.

3.2 Yöntem

1. Halka açık olan KDD'99 veri seti analizi yapıldı. Veri seti text olarak tutulmaktadır. Veri setinde bulunan tekrarlı veriler Java programlama dilinde yazılan kod ile elimine edildi.
2. Veri setinde bulunan alfanumerik değerler sayısal değerlere dönüştürüldü (Örnek: saldırı türü: buffer_overflow →1, neptune →9 vb)
3. İlgili veri seti analiz için SPSS programına yüklendi. SPSS programında bağımsız değişkenin bağımlı değişken üzerindeki etkisini ölçmek için linear regresyona tabi tutuldu.
4. Regresyon sonucunda oluşturulacak modelin karmaşıklığını azaltmak için bazı özellikler (giriş parametreleri) devre dışı bırakıldı.
5. Modelleme Matlab uygulamasında yapılmıştır. Modelleme algoritmaları olarak Yapay Sinir Ağları ve Karar Ağaçları kullanılmıştır.
6. Kullanılan yapay sinir ağları modelinin en başarılı sonucunu bulmak için gizli katman sayılarında değişiklikler yapıldı. Ayrıca yapay sinir ağları algoritmalarından olan Levenberg-Marquard ve Bayesian Regularization karşılaştırıldı.
7. Veri seti içinde olmayan fakat var olan saldırı türlerinden yola çıkarak yeni çıktı değerleri eklendi. Bunlar:

Saldiri: Bağlantının saldırı olup olmadığını ortaya koymaktadır (1: Evet, 0: Normal Bağlantı) .

Ust_Saldiri: Yapılan saldırının grubu (0=DoS, 1=U2R, 2=R2L, 3=Probe, 4=Normal)

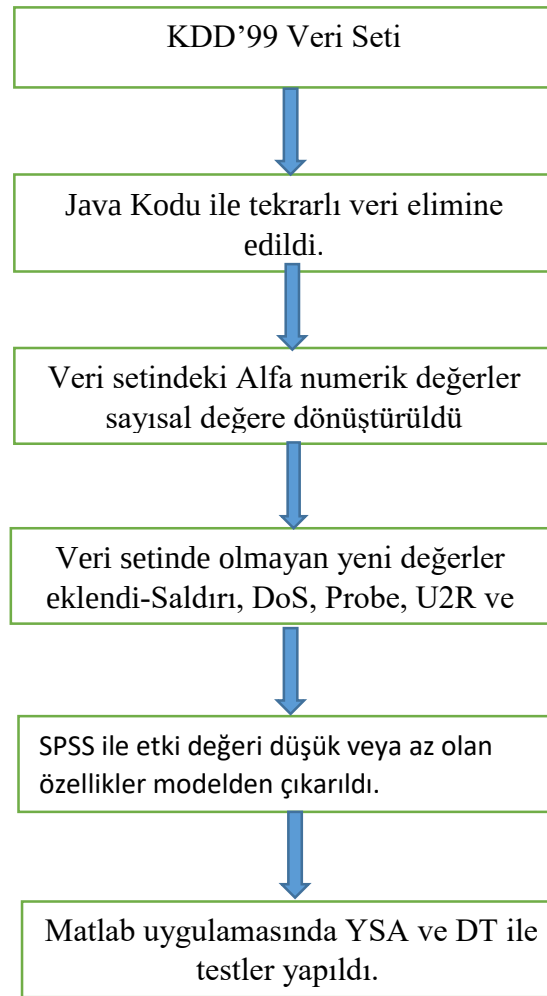
DoS: Bağlantının DoS saldırısı olup olmadığını ortaya koymaktadır (1: Evet, 0: Hayır).

U2R: Bağlantının U2R saldırısı olup olmadığını ortaya koymaktadır (1: Evet, 0: Hayır).

R2L: Bağlantının R2L saldırısı olup olmadığını ortaya koymaktadır (1: Evet, 0: Hayır).

Probe: Bağlantının Probe saldırısı olup olmadığını ortaya koymaktadır (1: Evet, 0: Hayır).

8. Regresyon neticesinde, seçilen giriş parametreleriyle gizli katman sayılarındaki değişimin modelin başarı oranı üzerindeki etkisi ölçülmüştür.
9. Seçilen özelliklerle sınıflandırma algoritmalarından olan karar ağacı ile test edilmiştir. Yapay Sinir Ağları ve Karar Ağaçları algoritmasına ait veriler karşılaştırılmıştır.
10. KDD'99 veri seti üzerinde diğer araştırmacıların yapmış oldukları modellemeler ile bu çalışmadaki sonuçlar karşılaştırılmıştır.



Şekil 3.4. Uygulanan sistem mimarisi.

3.2.1 Öğrenme Algoritmaları

3.2.1.1. Gözetimli-Eğitilmiş-Denetimli Öğrenme (Supervised Learning)

Gözetimli öğrenmede daha önce elde olan ve etiketlenmiş veri olur. Eğitilmiş Öğrenme algoritmalarında mevcut veri setinde eğitilir ve yeni girdiler için sonuç tahmin edilir.

Denetimli öğrenme teknikleri regresyon ve sınıflandırma olarak iki türe ayrılabilir.

Elimizde Batman iline ait belli giriş parametrelerine göre fiyat listesi olan veri seti olsun buna karşılık yeni bir evin fiyatını tahmin etmemiz istendiğinde regresyon metodunu kullanırız.

Buna karşın gene elimizde belli özellik değerlerine sahip (yaş, büyüklük vb.) tümörlerin iyi huylu ya da kanser olup olmadığı ile ilgili veri seti olsun. Yeni bir tümör tespit edildiğinde bunun iyi huylu ya da kötü huylu olmasını tahmin etmemiz gerektiğinde ise sınıflandırma yapmış oluruz.

Denetimli öğrenme algoritmaları aşağıdaki gibidir:

- Decision Trees- Karar Ağaçları
- K Nearest Neighbors- K En Yakın Komşu
- Linear SVC (Support vector Classifier) – Doğrusal Destek Vektör Sınıflandırıcı
- Logistic Regression – Doğrusal Regresyon
- Naive Bayes – Genel Bayes
- Neural Networks- Nöral Ağlar
- Linear Regression – Doğrusal Regresyon
- Support Vector Regression (SVR)
- Regression Trees (Random Forest) – Regresyon Ağaçları
- Gradient boosting – Gradyan Artırma
- Fisher linear discriminant – Fisher Doğrusal Ayırt Edici

3.2.1.2. Gözetimsiz-Eğitimsiz-Denetimsiz Öğrenme (UnSupervised Learning)

Denetimsiz öğrenme algoritmaları insan rehberliği olmadan hareket eder. Eldeki veri seti denetimli öğrenmede olduğu gibi etiketlenmemiştir. Denetimsiz Öğrenme, kullanılan algoritmadan verinin benzerliği ve farklılıklarından yola çıkarak gruplandırma işlemi yapar.

Denetimsiz öğrenmede makinenin gizli yapıyı kendi başına ortaya çıkarması beklenir. Eğitimli öğrenme olarak tanımlanmasının nedeni giriş parametrelerine karşılık bir sonuç tanımlanmamış olmasıdır.

Denetimsiz öğrenme, Kümeleme (Clustering) ve İlişkilendirme (Association) olmak üzere iki temel yöntem ile yapılmaktadır.

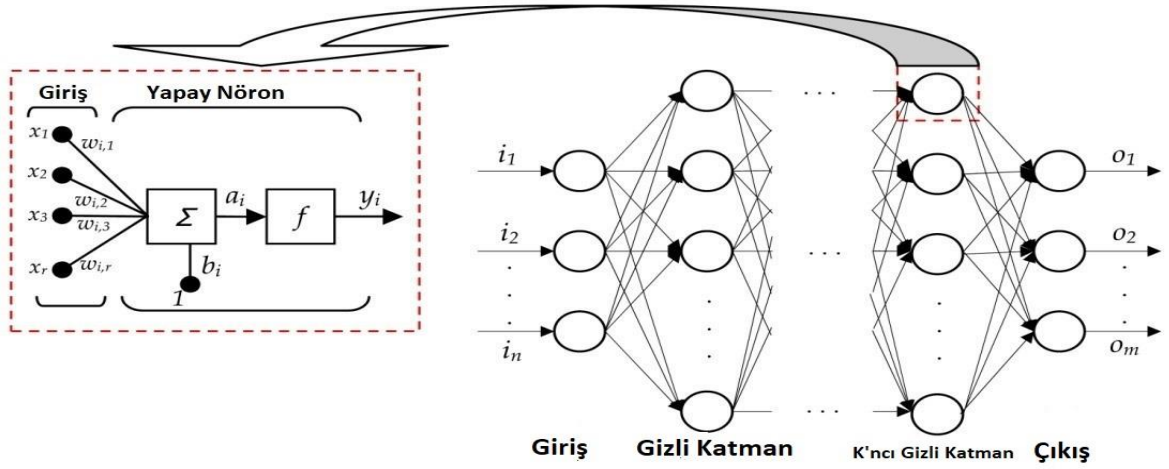
1. Kümeleme: Veri setindeki verileri benzerliklerine göre daha küçük kümelere bölme işlemidir.
2. İlişkilendirme (Association): Veri seti içerisindeki veriler arasında ilişki kurma yöntemidir. Örnek olarak A şarkıcısına ait şarkıyı dinleyen B şarkıcısına ait şarkıyı da dinlemesi.

Eğitimsiz Öğrenme algoritmaları ve teknikleri aşağıdaki gibidir:

- K-means clustering – K means kümeleme
- K-NN (k nearest neighbors) – K En Yakın Komşu
- Dimensionality Reduction – Boyutsal küçülme
- Neural networks / Deep Learning – Sinir ağları / Derin Öğrenme
- Principal Component Analysis – Temel bileşenler Analizi
- Singular Value Decomposition – Tekil Değer Ayrışımı
- Independent Component Analysis – Bağımsız Bileşen Analizi
- Distribution models – Dağıtım modelleri
- Hierarchical clustering – Hiyerarşik kümeleme
- Mixture models – Karışım modelleri

3.2.1.3. Kullanılan Algoritmalar

3.2.1.3.1 Artificial Neural Network- Yapay Sinir Ağlar



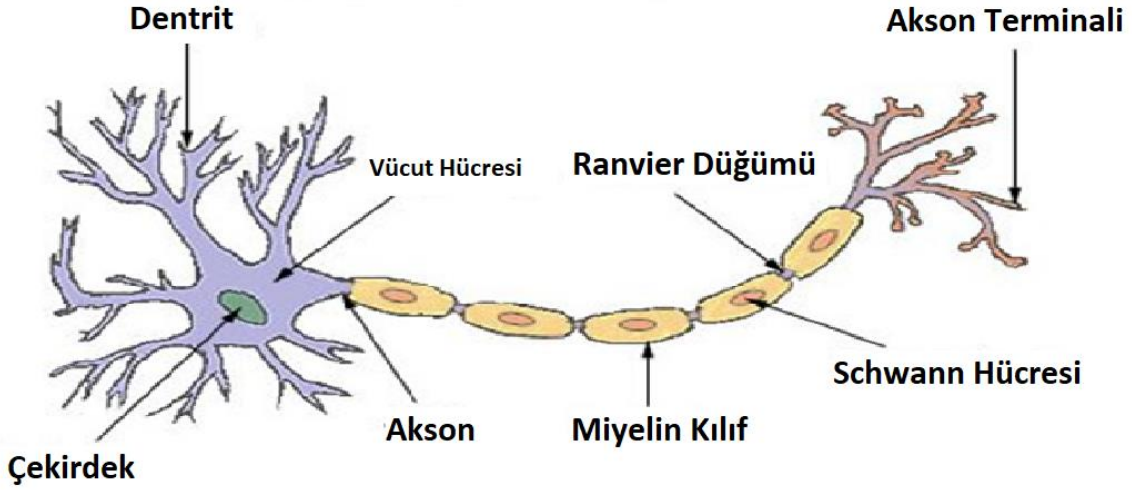
Şekil 3.5. YSA Çalışma Prensibi (Jain, 2016).

Yapay Sinir Ağları (YSA) genellikle sinir ağları olarak tanımlanır. Yapay Sinir Ağlarının modellenmesi hayvan beyinlerinden ilham alınmıştır.

Sinir ağlarında girdi ve çıktı katmanları dışında verilen girdiyi çıktı katmanında kullanılabileceği gizli katmanlar (hidden layer) bulunmaktadır.

Warren McCulloch ve Walter Pitts tarafından 1943 yılında sinir ağları için hesaplama modeli oluşturulmuştur (Hebb ve ark., 1949). İlk fonksiyonel ve çok katmanlı sinir ağı 1965 yılında Ivakhnenko and Lapa tarafından Grup veri İşleme Yöntemi olarak yayınlandı (Schmidhuber, 2015) (Ivakhnenko ve ark., 1965).

YSA biyolojik bir beyindeki sinir hücrelerini serbest bir şekilde modelleyen, yapay sinir hücreleri olarak tanımlanan bağlı birimler veya düğümlerin ilişkilendirilmiş haline dayanır. İnsan ya da hayvan beyinlerindeki sinapslar gibi her bir bağlantı başka sinir hücresine aktarılabilir. Bir sinyal alan yapay bir nöron, aldığı veriyi işler ve kendisine bağlı olan diğer nöronlara iletebilir.



Şekil 3.6. Bir nöronun yapısı (Jain, 2016).

Biyolojik öğrenme nöronlar arasındaki sinaptik bağlantıların oluşumuyla gerçekleşir. Canlılarda öğrenme yaşanan tecrübelerle öğrenirler. YSA öğrenme de buna benzemektedir. Öncelikle algoritmanın öğrenmesi için girdi ve çıktılar verilir. Bu şekilde girdi ve çıktı arasında bir bağlantı oluşturulur. Bu işlem çok defa tekrar edilir.

Geleneksel işlem birimlerinde var olan problem merkezi bir şekilde ele alınırken YSA’larda birden fazla basit işlem birimi bulunmaktadır. Problemin tamamı bu işlem birimleri arasında paylaştırılmakta ve kendilerinde verilen işin yapılması beklenmektedir.

YSA Avantajları (Mijwel, 2018):

1. Bilgiyi Saklama Yöntemi:

Geleneksel programlarda veriler bir veri tabanında tutulurken YSA’larda veriler ağıın tamamında tutulur. Bu verilerde birkaçının kaybolması çalışmayı engellemez.

2. Eksik Bilgi ile Çalışabilme:

YSA’da ağıın eğitilmesi sonrası ağıa verilecek yeni girdilerde eksik olması durumunda bile çıktı üretebilmektedir. Eksik girdilerin önemi ağıın performansı etkilemektedir.

3. Hata Toleransı:

YSA'da giriş parametrelerinde bir veya daha fazla parametrenin bozulması durumunda bile bir sonuç üretir. Bu özellik ağın hata dayanaklığını güçlendirir.

4. Aynı Anda İşlem Yapabilme:

Geleneksel programlarda aynı anda tek bir işlem yapılabilirken YSA'da aynı anda birden fazla işlem yapabilme yeteneğine sahiptir.

5. Kendi Kendine Öğrenme:

Yapay Sinir Ağları daha önce gerçekleşmiş olaylardan öğrenir ve benzer olaylar hakkında karar verebilir.

6. Dağıtılmış Hafıza:

YSA'nın öğrenebilmesi için örneklerin belirlenmesi ve ağı eğitilmesi gerekmektedir. YSA'da doğru örneklerin seçilmesi başarı şansını artırır. Ağa doğru örnekler verilmemesi durumunda ise çıktıların hatalı çıkma ihtimali yükselir.

7. Aşamalı Bozulma:

Bir ağ zamanla yavaşlar ve bozulmaya uğrar.

YSA Dezavantajları (Mijwel, 2018):

1. Donanım Gereksinimleri

Yapay Sinir Ağlarında işlemler paralel olarak yürütüldüğünden yüksek performanslı işlemcilerle ihtiyaç duyulmaktadır.

2. Anlaşılmamış Hata

YSA verilen girdilerle bir sonuç ürettiğinde bu sonucu nasıl ve neden verdiği ile ilgili bilgi vermez. Bu da Yapay Sinir Ağlarının en önemli problemlerinden bir tanesidir.

3. Uygun Ağ Belirlenmesi

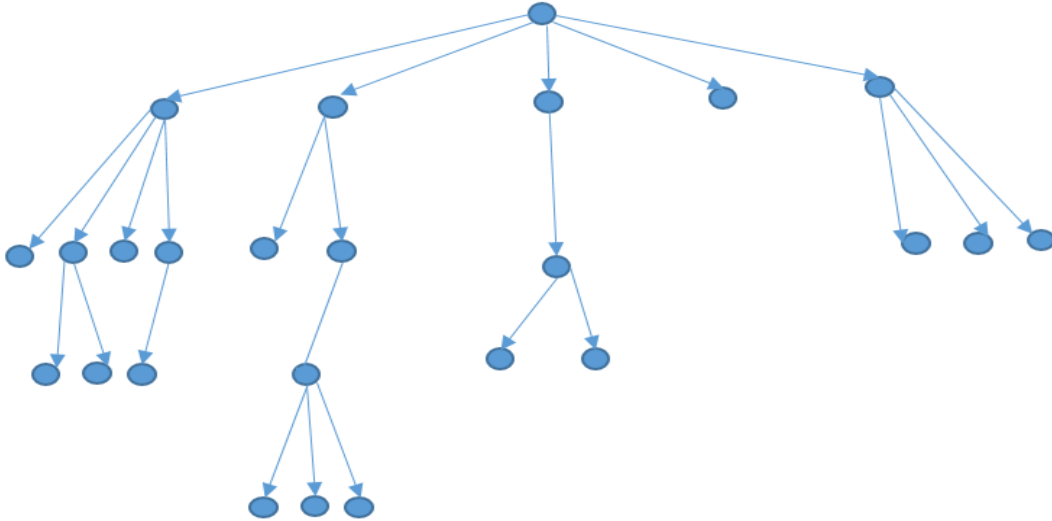
Yapay Sinir Ağlarının yapısını belirlemek için sabit kurallar bulunmamaktadır. Uygun yapıyı belirlemek için tecrübe ve denemelere başvurulur.

4. Verinin Ağın Anlayabileceği Şekle Dönüştürme

Yapay Sinir Ağları sayısal veriler ile çalışmaktadır. Dolayısı ile eldeki verilerin YSA'nın anlayabileceği şekle dönüştürülmesi ve bu işlemin titizlikle yapılması ağın performansını büyük ölçüde etkilemektedir.

3.2.1.3.2 Decision Trees (Karar Ağaçları)

Karar ağaçları, veri biliminde sınıflandırma ve tahminde çokça kullanılan tekniklerden bir tanesidir (Çalış ve ark., 2014). Karar ağacı, ağaç benzeri bir karar modelini ve bunların olası sonuçlarını kullanan bir karar mekanizmasıdır (Anonymous, 2020). Koşullu durumlar için kullanılan makine öğrenmesi algoritmalarından bir tanedir.



Şekil 3.7. Karar Ağacı Modeli

Karar ağacı, her dâhili düğümün bir öznitelik üzerinde bir "testi" temsil ettiği (örneğin, yazı mı tura mı gelir), her dal testin sonucunu temsil eden ve her yaprak düğümün bir sınıfı temsil ettiği akış şemasına benzer bir yapıdır.

Bir karar ağacı üç düğümden oluşur (Kamiński ve ark., 2017).

1. Karar Düğümleri – Kareler ile temsil edilir
2. Şans Düğümleri – Daireler ile temsil edilir
3. Uç Düğümler – Üçgenlerle temsil edilir.

Karar ağaçları koşullu durumlar için sıkça kullanılan yöntemlerden bir tanedir.

Karar ağaçları öğrenmesinde, veri seti belli özelliklere göre alt kümelere ayrılır. Alt kümelere ayırma işlemi tekrarlanır. Bu işlem sonuç üzerinde etki etmeyecek kadar tekrarlanır. Bu işlem özyinele parçalama (recursive partitioning) olarak tanımlanır.

Sınıflandırma Ağaçları (Classification Trees): Kategorik sınıflandırma problemlerinde kullanılan yöntemdir. Çeşitli özelliklere göre tespit edilen kitlenin kötü huylu ya da iyi huylu tümör olduğunu tahmin etme gibi problemlerde kullanılabilir.

Regresyon Ağaçları (Regression Trees): Devamlılık arz eden problemlerin çözümünde başvurulan yöntemdir. Örneğin belli özelliklere göre ev fiyatlarının tahmininde başvurulan yöntemdir.

Karar Ağaçlarının kullanım alanları (Diepen ve ark., 2006).

- Kategorik sınıfların muhtemel üyesi olacak özelliklerin belirlenmesi,
- Belli durumlarda yüksek, orta ve düşük risk grupları gibi belli başlı kategorilere ayrılması,
- Parametrik modellerin kurulmasında kullanılmak üzere çok sayıdaki değişkenden en önemlilerinin seçilmesi,
- İleriki olayların tahmin edilmesine yönelik kurallar oluşturulması
- Alt grupların tabi tutulacağı ve sadece o grubu etkileyen ilişkilerin tanımlanması,
- Belli başlı kategorilerde birleştirme işlemin yapılması yanında değişkenlerin alt değişkenlere çevrilmesidir.

Karar Ağaçlarının Avantajları

- Karar ağacı modelinin anlaması ve yorumlamak çok kolaydır.
- Küçük bilgi girişlerinde bile bir çıkış verisi elde edilebilmektedir.
- Farklı senaryolar için en kötü, en iyi ve beklenen değerlerin belirlenmesine yardımcı olur.
- Diğer teknikler ve algoritmalarla birleştirilebilir.

Karar Ağaçları Dezavantajları

- Veri setindeki küçük bir değişiklik algoritmada çok büyük değişikliğe neden olabilir dolayısı ile stabil değildir.

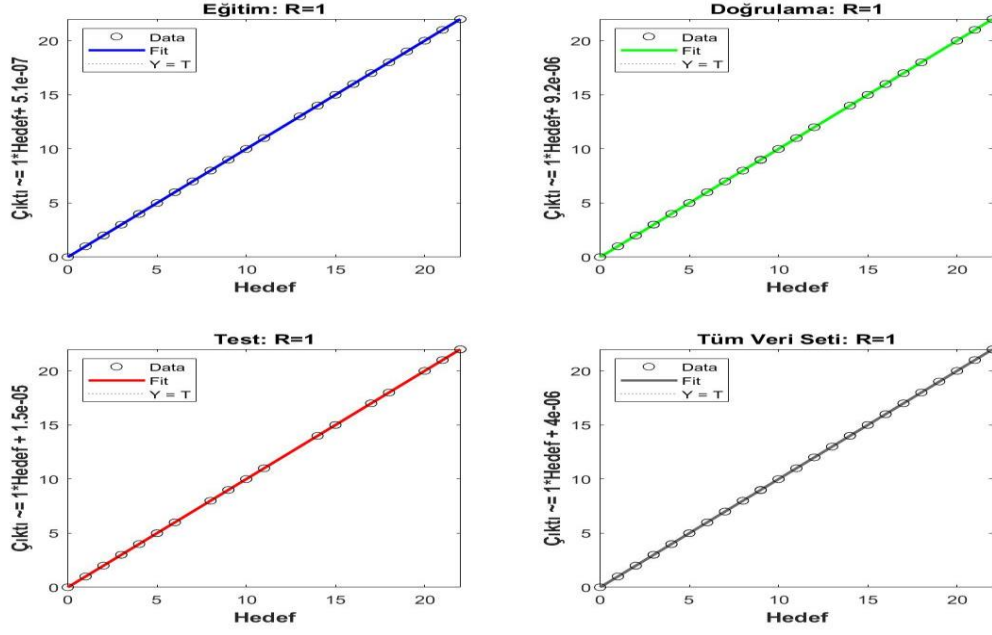
- Diğer yöntemlere göre karar ağacı algoritması performans ve doğruluk oranı olarak daha kötüdür.
- Farklı sayıda seviyeye sahip kategorik değişkenler içeren veriler için, karar ağaçlarındaki bilgi kazanımı, daha fazla seviyeye sahip öznitelikler lehine önyargılıdır (Deng ve ark., 2011).
- Birçok değer belirsiz veya birçok sonuçla bağlantılıysa hesaplama algoritması çok komplike hale gelir.

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

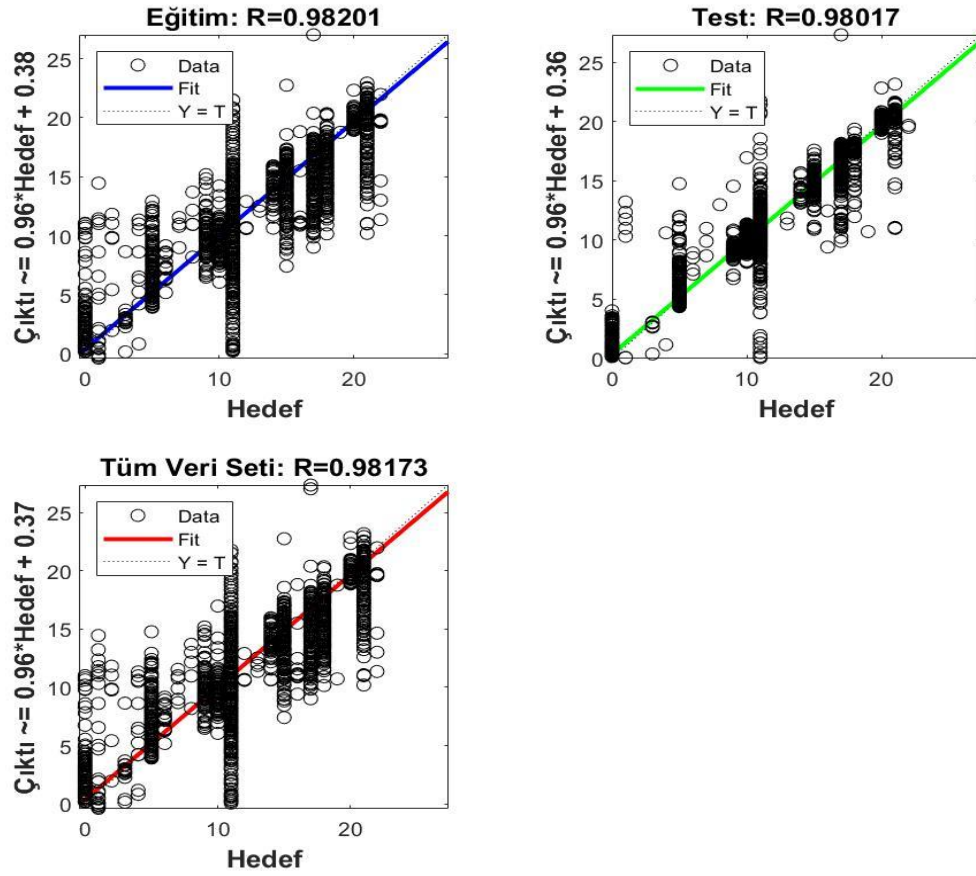
Bu bölümde Tez'in deneysel çalışma sonuçları açıklanmış olup literatüre katkıları irdelenmiştir. Tablo 4.1 'de aynı parametreler ile Levenberg-Marquard ve Bayesian Regularization algoritmaları sistem kaynağı tüketimi ve modelin öğrenme süresi konularında test edilmiştir.

Tablo 4.1. Levenberg-Marquard Bayesian Regularization Karşılaştırılması

Levenberg-Marquard Bayesian Regularization Karşılaştırılması		
Giriş Parametre Adeti	41	41
Gizli Katman Sayısı	10	10
Öğrenme Algoritması	Levenberg-Marquard	Bayesian Regularization
Epoch	41	1000
Süre	00:04:48	01:09:24
Eğitim Veri Seti Örnek Sayısı	734001	734001
Doğrulama Veri Seti Örnek Sayısı	157286	
Test Veri Seti Örnek Sayısı	157286	157286
Eğitim Veri Seti MSE	0,0648	0,0467
Doğrulama Veri Seti MSE	0,0879	0
Test Veri Seti MSE	0,0734	0,0531
Eğitim Veri Seti R	0,978	0,984
Doğrulama Veri Seti R	0,97	0
Test Veri Seti R	0,974	0,982



Şekil 4.1. YSA Levenberg-Marquard öğrenme algoritması plot regresyon grafiği



Şekil 4.2. YSA Bayesian Regularization öğrenme algoritması plot regresyon grafiği

Yukardaki tabloda aynı parametreler ve aynı gizli katman sayısı ile yapılan iki farklı algoritmanın sonucu verilmiştir.

Levenberg-Marquard algoritması ile yapılan öğrenmede bellek ihtiyacı Bayesian Regularization algoritmasına göre daha fazladır. Buna karşın daha hızlı şekilde sonuç alınmaktadır.

Yukarda gösterilen tabloda aynı giriş parametresi, aynı gizli katman ve çıkış parametresi ile yapılan öğrenmede Levenberg-Marquard algoritması 4 dakika 48 saniye gibi bir süre alırken beri tarafta Bayesian Regularization algoritması ile yapılan öğrenme ise 1 saat 9 dakika 24 saniye sürmüştür.

Levenberg-Marquard algoritması 41 iterasyonda optimal değere ulaşırken Bayesian Regularization algoritması ise doğrulama işlemine başvurmamakta ve maksimum değer olan 1000 iterasyona kadar devam etmektedir.

Bayesian Regularization algoritması daha fazla zaman gerektirir. Ancak zor, küçük veya gürültülü veri kümeleri için iyi sonuçlar elde edilebilir. Uyarlanabilir ağırlık minimizasyonuna göre eğitim durur.

Bir modelin tahmin doğruluğunu ölçmek için kullanılan en yaygın ölçümlerden biri, ortalama hata karesi anlamına gelen mean square error (MSE)'dir. Yukardaki tablo göz önüne bulundurulduğunda Bayesian Regularization algoritması yapılan öğrenmenin Levenberg-Marquard algoritmasına göre daha başarılı olduğu tespit edilmiştir.

R değerinin 1'e yakın olması algoritmanın başarılı olduğu anlamına gelmektedir. Levenberg-Marquard algoritması ve Bayesian Regularization algoritması karşılaştırıldığında eğitim test ve tümünün ortalamasını gösteren şekiller göz önünde bulundurulduğunda Bayesian Regularization algoritmasının daha başarılı olduğu ortaya çıkmaktadır.

Tablo 4.2. Farklı Gizli Katman Sayılarıyla Sonuçların Karşılaştırılması

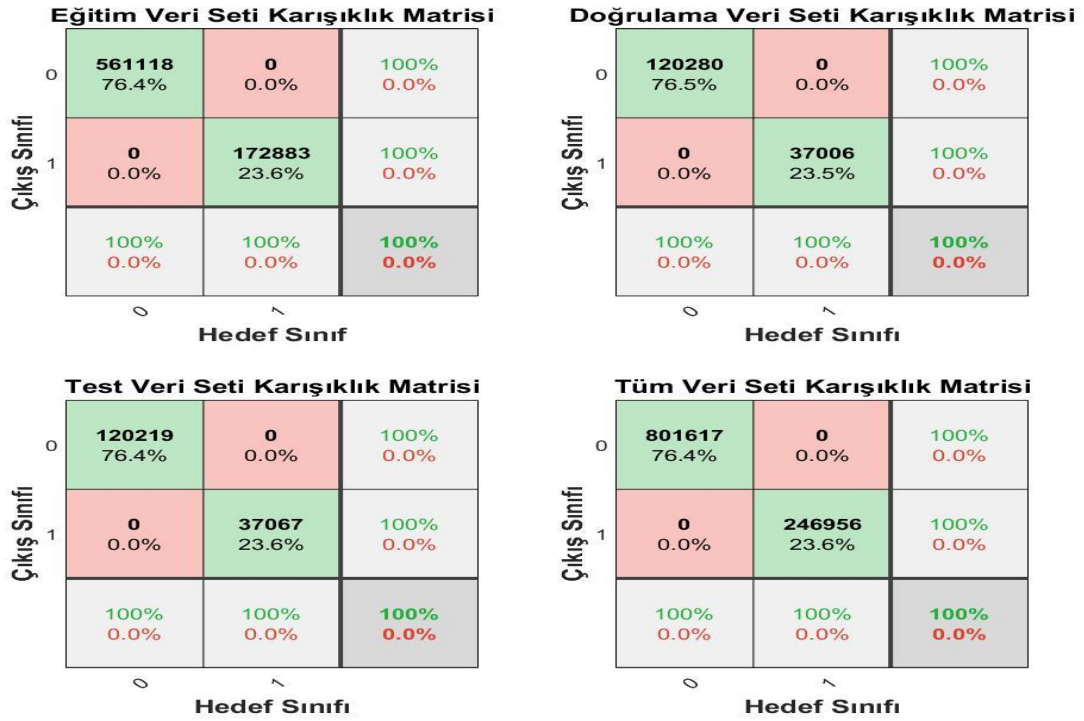
Farklı Gizli Katman Sayılarıyla Sonuçların Karşılaştırılması				
Gizli Katman Sayısı	10	15	30	50
Giriş Parametre Adeti	41	41	41	41
Öğrenme Algoritması	Levenberg-Marquard	Levenberg-Marquard	Levenberg-Marquard	Levenberg-Marquard
Epoch	41	101	84	88
Süre	00:04:48	00:10:01	00:20:01	01:00:06
Eğitim Veri Seti Örnek Sayısı	734001	734001	734001	734001
Doğrulama Veri Seti Örnek Sayısı	157286	157286	157286	157286
Test Veri Seti Örnek Sayısı	157286	157286	157286	157286
Eğitim Veri Seti MSE	0,0648	0,0456	0,049	0,0414
Doğrulama Veri Seti MSE	0,0879	0,0563	0,647	0,0526
Test Veri Seti MSE	0,0734	0,0773	0,534	0,103
Eğitim Veri Seti R	0,978	0,984	0,983	0,986
Doğrulama Veri Seti R	0,973	0,981	0,978	0,982
Test Veri Seti R	0,974	0,974	0,981	0,965

Yukardaki tabloda 10, 15, 30 ve 50 gizli katman sayılarının sonuç üzerindeki etkisi ortaya konulmuştur.

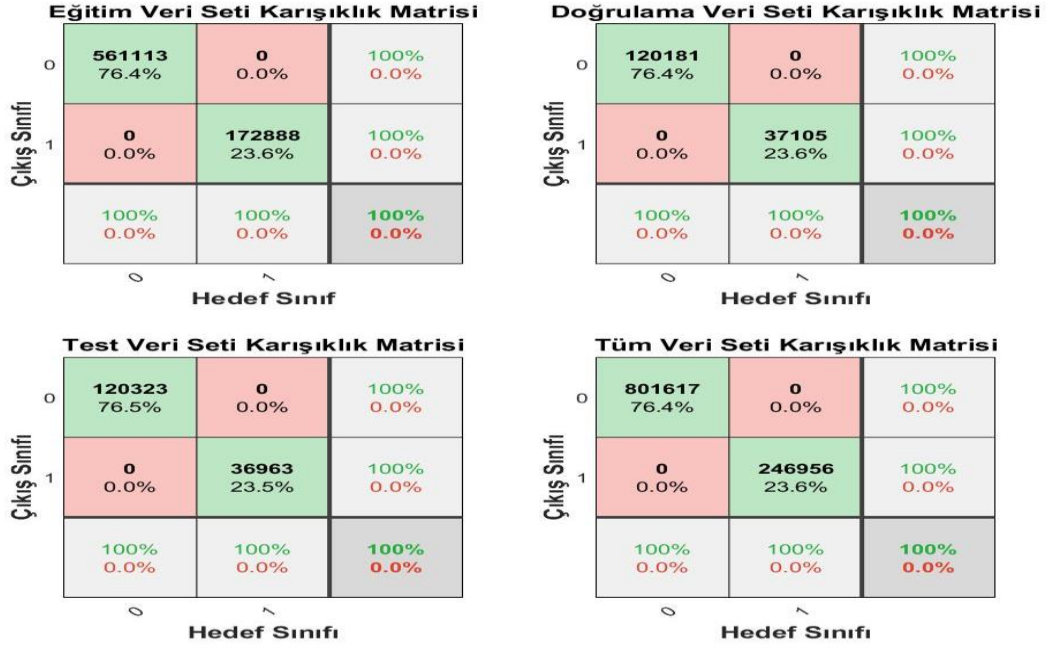
Yukardaki veriler göz önünde bulundurulduğunda aşağıdaki sonuçlar elde edilir.

- Farklı nöronlarla yapılan training- eğitim veri seti üzerinde yapılan modellemede en uygun olan 50 gizli katmanlı modeldir.
- Doğrulama veri seti üzerinde yapılan modellemede en uygun olan 50 gizli katmanlı modeldir

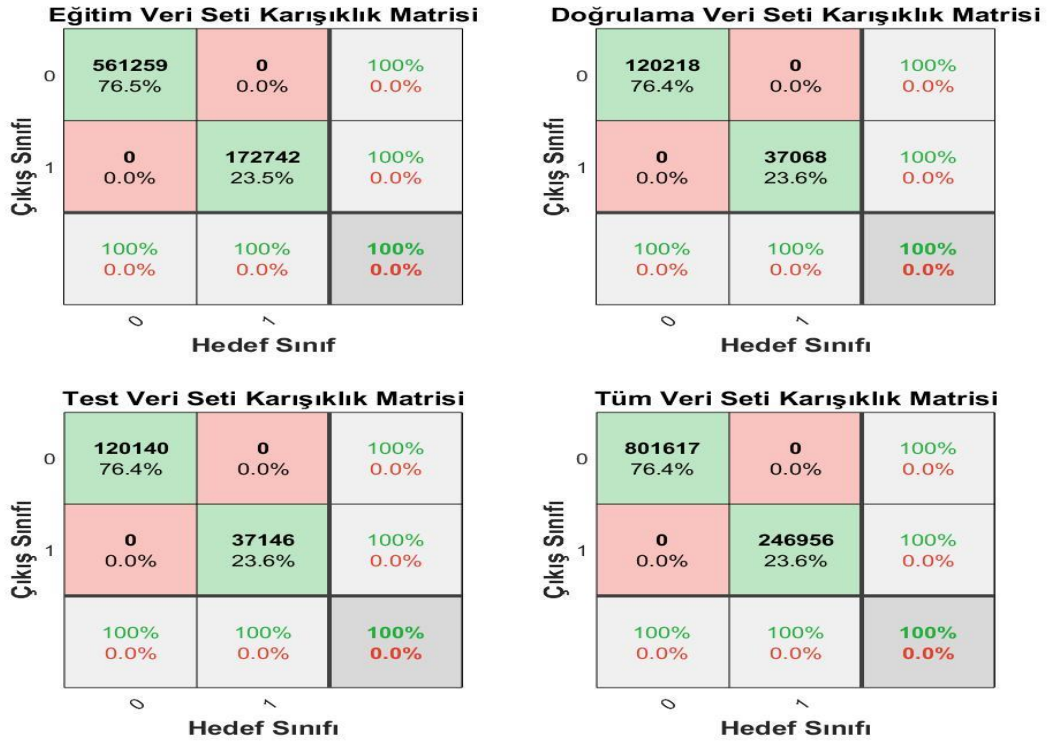
- Test veri seti üzerinde eğitim ve doğrulama sonucu elde edilen modelde yapılan testte en başarılı olan 30 gizli katmanlı modeldir.
- Eğitim ve Doğrulama veri setinden yapılan öğrenmede en iyi sonucu 50 gizli katmanlı yapıdan elde edilirken buna karşın modelin test edildiğinde 30 gizli katmanlı modelde daha başarılı sonuç vermesi 50 katmanlı modelde bir yerden sonra öğrenmeden çok ezberlemenin söz konusu olduğunu bize göstermektedir.
- Modeldeki epoch sayısı gizli katman sayısı ile orantılı değildir.
- Optimal modelin oluşturulmasında, gizli katman sayısı ile zaman arasında doğrusal bir orantı mevcuttur.



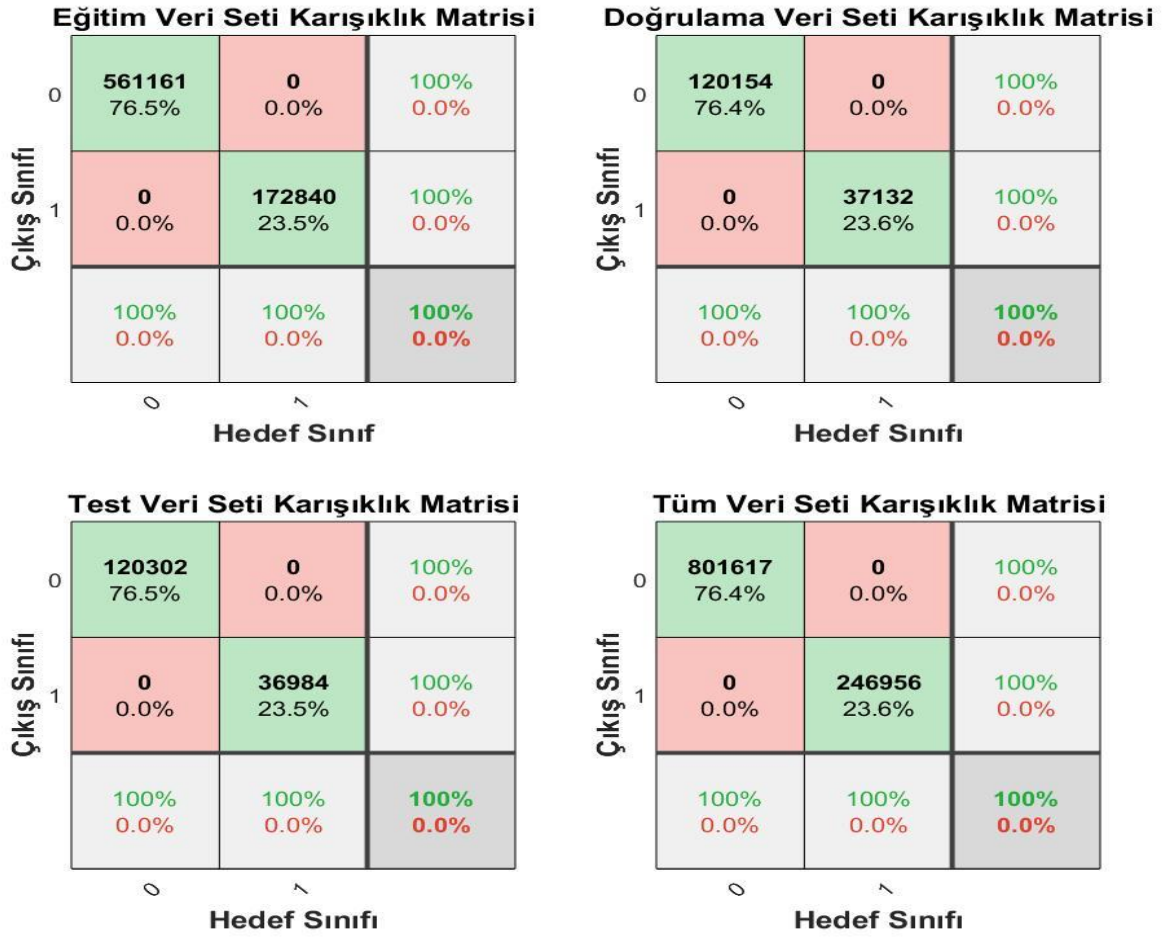
Şekil 4.3. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 10 gizli katmanlı (0: Saldırı Değil, 1: Saldırı)



Şekil 4.4. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 15 gizli katmanlı (0: Saldırı Değil, 1: Saldırı)



Şekil 4.5. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 30 gizli katmanlı (0: Saldırı Değil, 1: Saldırı)



Şekil 4.6. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 50 gizli katmanlı (0: Saldırı Değil, 1: Saldırı).

Eğitim veri seti, modelin eğitilmesinde kullanılan veri setidir.

Doğrulama veri seti, oluşturulmuş modeldeki hiperparametreler ayarlanırken uygun modelin tarafsız bir değerlendirmesini sağlamak için kullanılan veri setidir. Oluşturulan modelin değerlendirilmesi için kullanılır. Kullanılan hiperparametrelerin uygunluğu için bu veri setinde başvurulur ve kontrol işlemine tabi tutulur. Fakat bu veri setinde öğrenme olmaz. Sonuç olarak Doğrulama veri seti oluşturulan modelin geliştirilmesi için kullanılır.

Test veri seti, eğitim veri setine uyan nihai modelin tarafsız bir değerlendirmesini sağlamak için kullanılan veri setidir. Test veri kümesi, eğitim ve doğrulama veri setini kullanarak elde edilen modeli değerlendirmek için kullanılan veri setidir.

Yukardaki veriler göz önünde bulundurulduğunda aşağıdaki sonuçlar elde edilir.

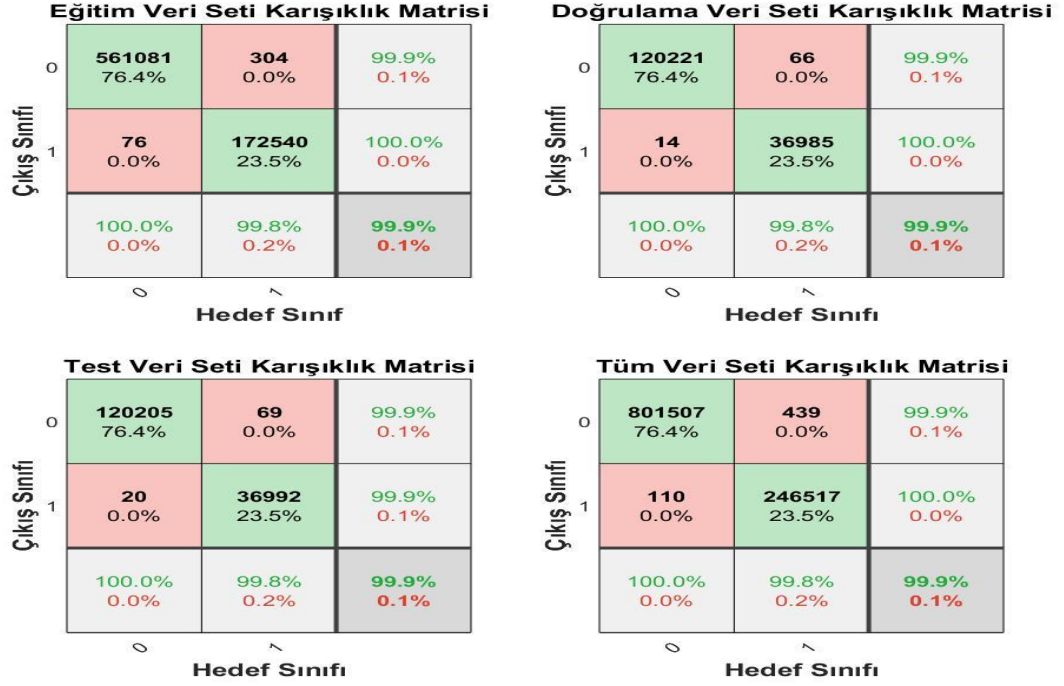
- Yukardaki şekillerde farklı nöron sayılarındaki değerler göz önünde bulundurulduğunda gelen bağlantının saldırı olup olmadığı ile ilgili oluşturulan modelin gizli katman sayısından bağımsız hepsini doğru tahmin edebildiğini görmekteyiz.
- Modelin eğitilmesinde seçilen özellikler modelin performansını etkilemektedir.

Tablo 4.3. Eliminasyon sonrası elde edilen sonuçlar

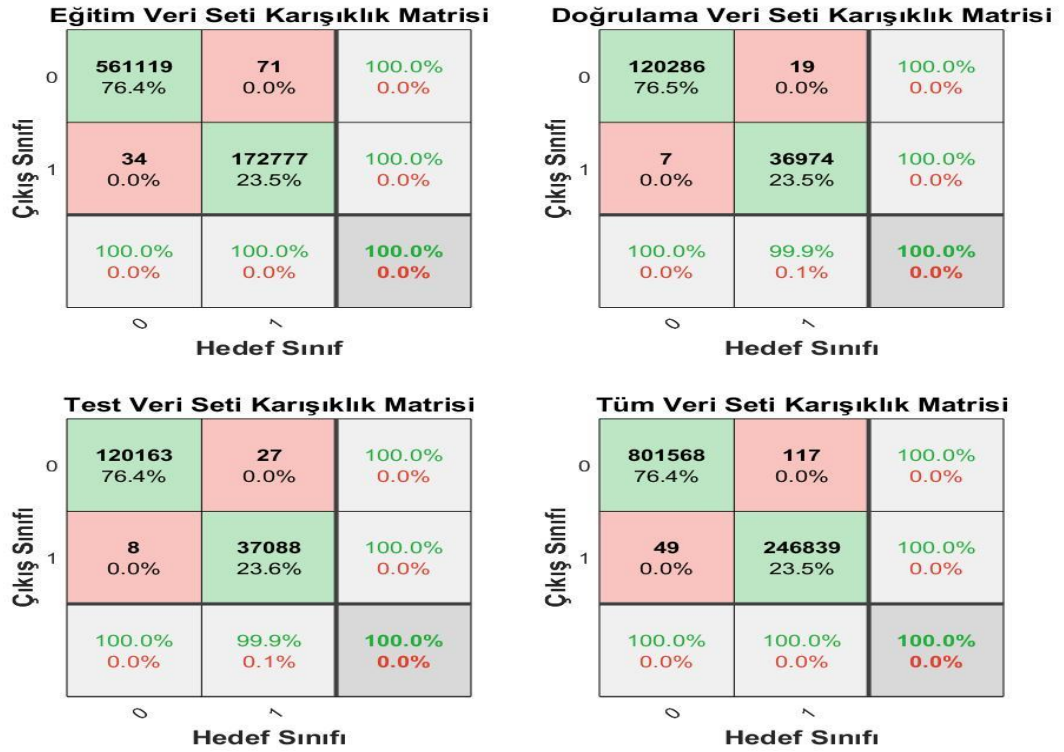
Eliminasyon** sonrası elde edilen sonuçlar				
Gizli Katman Sayısı	10	15	30	50
Giriş Parametre Âdeti	35	35	35	35
Öğrenme Algoritması	Levenberg-Marquard	Levenberg-Marquard	Levenberg-Marquard	Levenberg-Marquard
Epoch	105	179	109	85
Süre	00:06:10	00:14:50	00:21:00	00:37:00
Eğitim Seti Örnek Sayısı	734001	734001	734001	734001
Doğrulama Seti Örnek Sayısı	157286	157286	157286	157286
Test Seti Örnek Sayısı	157286	157286	157286	157286
Eğitim MSE	0,0609	0,0456	0,04	0,0527
Doğrulama MSE	0,0879	0,0563	0,498	0,0694
Test MSE	0,0705	0,0773	0,512	0,0688
Eğitim R	0,979	0,984	0,986	0,982
Doğrulama R	0,976	0,981	0,983	0,976
Test R	0,977	0,974	0,982	0,977
** Elimine edilen parametreler: flag, su_attempted, num_file_creations, num_shells, num_access_files ve is_host_login				

Tablodaki veriler göz önünde bulundurulduğunda aşağıdaki sonuçlar elde edilir.

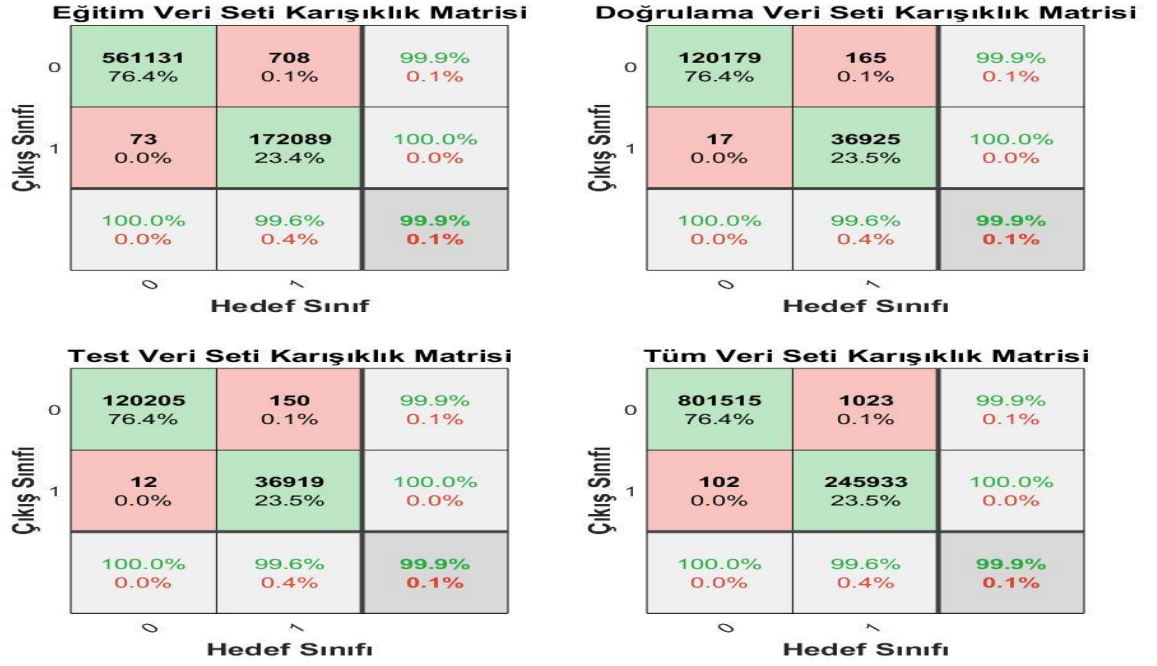
- Eğitim, Doğrulama ve Test veri seti üzerinde yapılan modellemede en iyi sonuçlar 30 gizli katmanlı modelde elde edilmiştir.
- Tablodaki veriler göz önünde bulundurulduğunda altı tane değişkenin modelden çıkarılması durumunda modelin karmaşıklığı azaldığı bununla birlikte sistem kaynağı ihtiyacı da azaldığı fakat buna karşın modelin doğruluk oranının düştüğü görülmektedir.



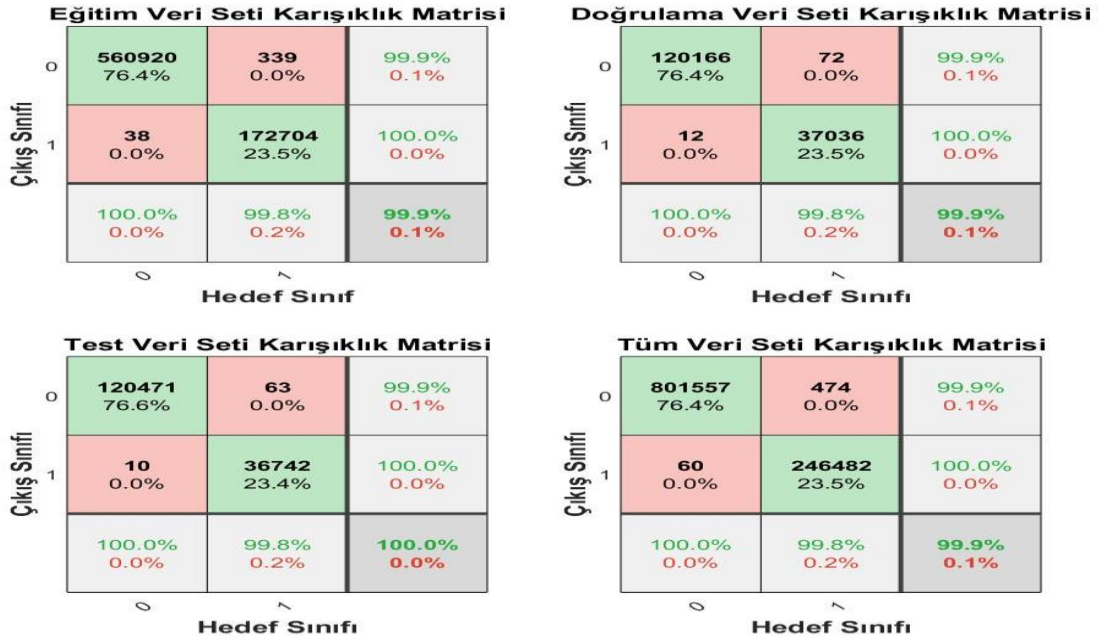
Şekil 4.7. Eliminasyon sonrası Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 10 gizli katmanlı (0: Saldırı Değil, 1: Saldırı)



Şekil 4.8. Eliminasyon sonrası saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 15 gizli katmanlı (0: Saldırı Değil, 1: Saldırı).



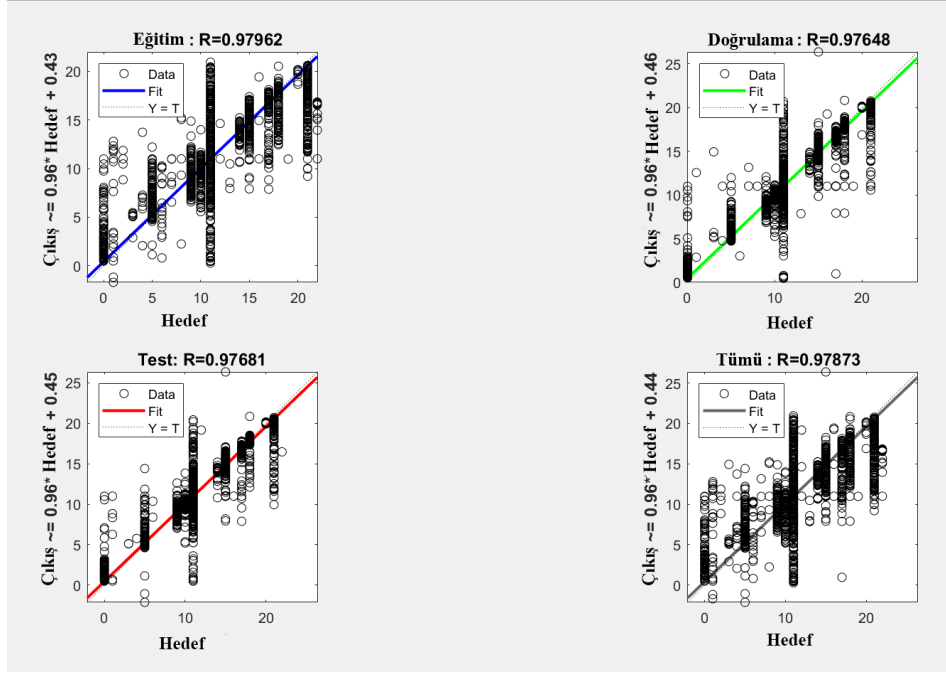
Şekil 4.9. Eliminasyon sonrası saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 30 gizli katmanlı (0: Saldırı Değil, 1: Saldırı)



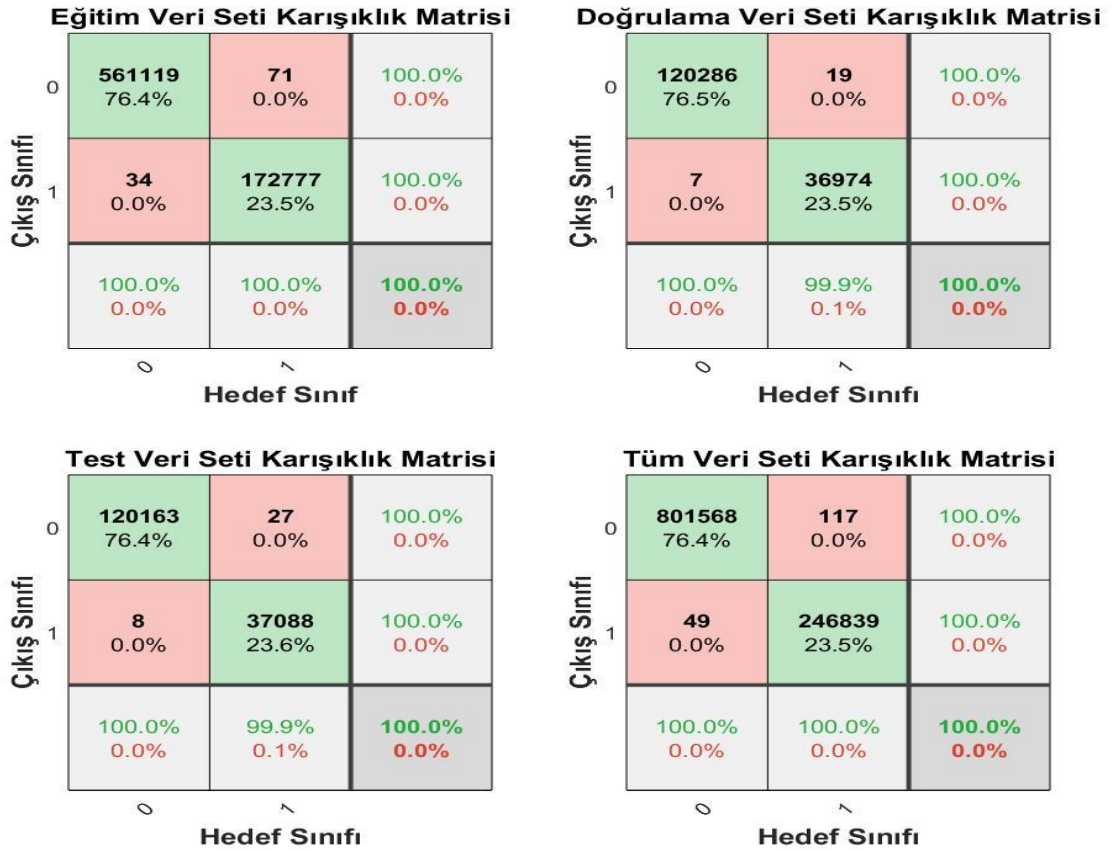
Şekil 4.10. Eliminasyon sonrası saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, 50 gizli katmanlı (0: Saldırı Değil, 1: Saldırı).

Tablo 4.4. 10 Gizli Katmanlı ve Farklı Çıkış Parametresine Göre Sonuçlar.

10 Gizli Katmanlı ve Farklı Çıkış Parametresine Göre Sonuçlar							
	Saldırı Türü	Saldırı	Saldırı Üst Türü	Dos	Probe	R2L	U2R
Giriş Parametre Âdeti	35						
Gizli Katman Sayısı	10						
Öğrenme Algoritması	Levenberg-Marquard						
Epoch	109	87	484	84	32	24	39
Süre	00:21:00	00:05:25	00:41:42	00:07:38	00:01:56	00:01:26	00:02:25
Eğitim Seti Örnek Sayısı	734001						
Doğrulama Seti Örnek Sayısı	157286						
Test Seti Örnek Sayısı	157286						
Eğitim MSE	0,00015	0,000179	0,006728	0,000107	0,000242	0,000032	0,000172
Doğrulama MSE	0,00021	0,000198	0,007285	0,000142	0,000331	0,000042	0,000206
Test MSE	0,00015	0,000988	0,007977	0,000199	0,000338	0,000017	0,000249
Eğitim R	0,9995	0,9995	0,9988	0,9997	0,9906	0,6328	0,9009
Doğrulama R	0,9993	0,9994	0,9987	0,9996	0,9875	0,4199	0,8869
Test R	0,9995	0,9972	0,9986	0,9994	0,9809	0,7049	0,8833



Şekil 4.11. Saldırı çıktısına ait plot regresyon grafiği (satan, neptune, vb).



Şekil 4.12. Saldırı olup olmadığına dair doğruluk ve karışıklık matrisi, (0: Saldırı Değil, 1: Saldırı).

Eğitim Veri Seti Karışıklık Matrisi

1	173194 23.6%	0 0.0%	2 0.0%	1 0.0%	27 0.0%	100.0% 0.0%
2	0 0.0%	7 0.0%	0 0.0%	3 0.0%	6 0.0%	43.8% 56.3%
3	15 0.0%	2 0.0%	9604 1.3%	0 0.0%	96 0.0%	98.8% 1.2%
4	0 0.0%	4 0.0%	0 0.0%	542 0.1%	109 0.0%	82.7% 17.3%
5	104 0.0%	22 0.0%	127 0.0%	133 0.0%	550003 74.9%	99.9% 0.1%
	99.9% 0.1%	20.0% 80.0%	98.7% 1.3%	79.8% 20.2%	100.0% 0.0%	99.9% 0.1%
	1	2	3	4	5	
	Hedef Sınıf					

Doğrulama Veri Seti Karışıklık Matrisi

1	36841 23.4%	0 0.0%	0 0.0%	0 0.0%	7 0.0%	100.0% 0.0%
2	0 0.0%	1 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
3	3 0.0%	0 0.0%	2030 1.3%	0 0.0%	28 0.0%	98.5% 1.5%
4	0 0.0%	1 0.0%	0 0.0%	126 0.1%	24 0.0%	83.4% 16.6%
5	26 0.0%	5 0.0%	25 0.0%	33 0.0%	118136 75.1%	99.9% 0.1%
	99.9% 0.1%	14.3% 85.7%	98.8% 1.2%	79.2% 20.8%	100.0% 0.0%	99.9% 0.1%
	1	2	3	4	5	
	Hedef Sınıf					

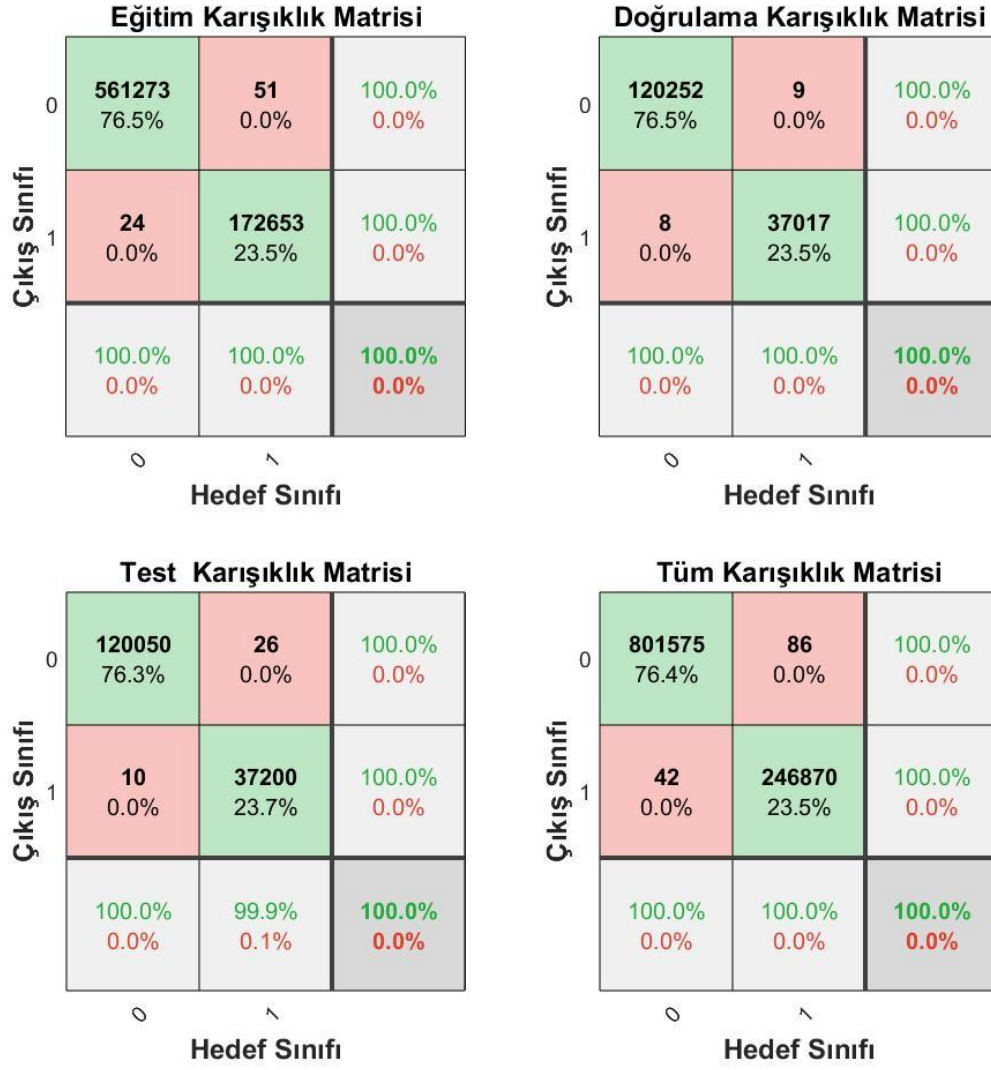
Test Veri Seti Karışıklık Matrisi

1	36735 23.4%	0 0.0%	1 0.0%	0 0.0%	4 0.0%	100.0% 0.0%
2	0 0.0%	5 0.0%	0 0.0%	0 0.0%	1 0.0%	83.3% 16.7%
3	6 0.0%	0 0.0%	2046 1.3%	1 0.0%	31 0.0%	98.2% 1.8%
4	2 0.0%	1 0.0%	0 0.0%	127 0.1%	32 0.0%	78.4% 21.6%
5	30 0.0%	4 0.0%	25 0.0%	33 0.0%	118202 75.2%	99.9% 0.1%
	99.9% 0.1%	50.0% 50.0%	98.7% 1.3%	78.9% 21.1%	99.9% 0.1%	99.9% 0.1%
	1	2	3	4	5	
	Hedef Sınıf					

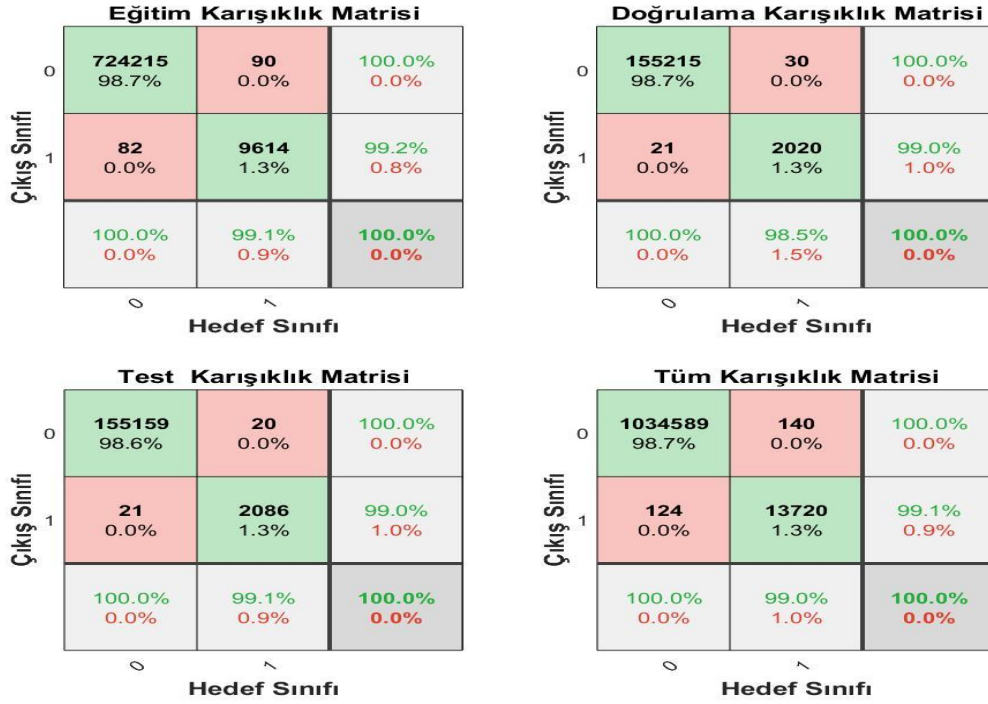
Tüm Veri Seti Karışıklık Matrisi

1	246770 23.5%	0 0.0%	3 0.0%	1 0.0%	38 0.0%	100.0% 0.0%
2	0 0.0%	13 0.0%	0 0.0%	3 0.0%	7 0.0%	56.5% 43.5%
3	24 0.0%	2 0.0%	13680 1.3%	1 0.0%	155 0.0%	98.7% 1.3%
4	2 0.0%	6 0.0%	0 0.0%	795 0.1%	165 0.0%	82.1% 17.9%
5	160 0.0%	31 0.0%	177 0.0%	199 0.0%	786341 75.0%	99.9% 0.1%
	99.9% 0.1%	25.0% 75.0%	98.7% 1.3%	79.6% 20.4%	100.0% 0.0%	99.9% 0.1%
	1	2	3	4	5	
	Hedef Sınıf					

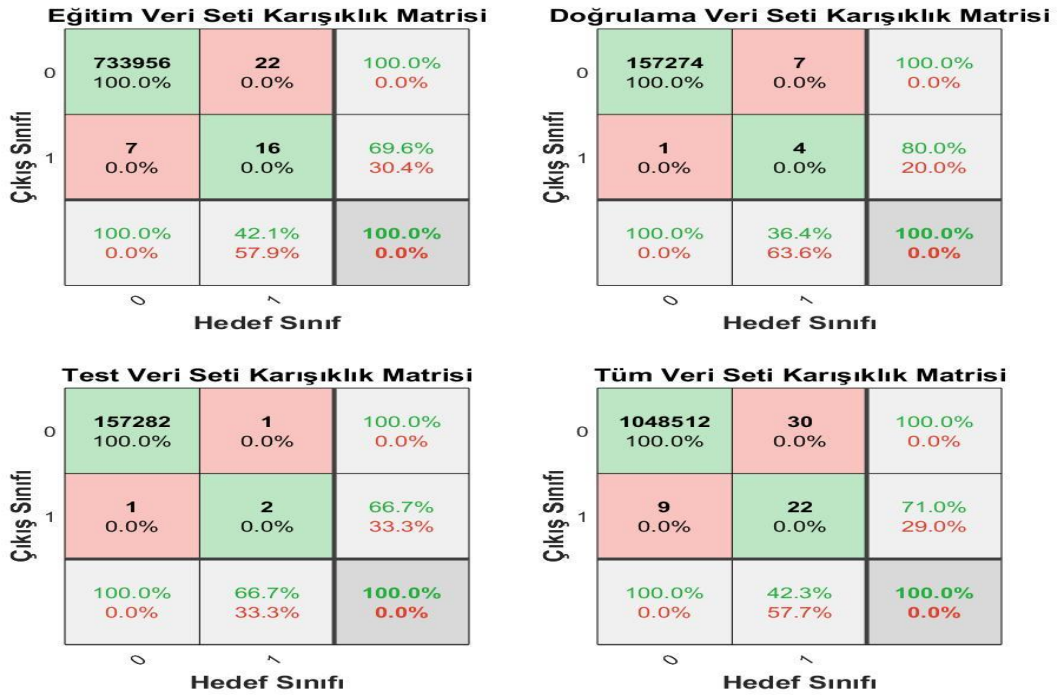
Şekil 4.13. Saldırı türüne ait doğruluk ve karışıklık matrisi, (1: DoS, 2: R2L, 3: Probe, 4: U2R, 5: Normal Bağlantı).



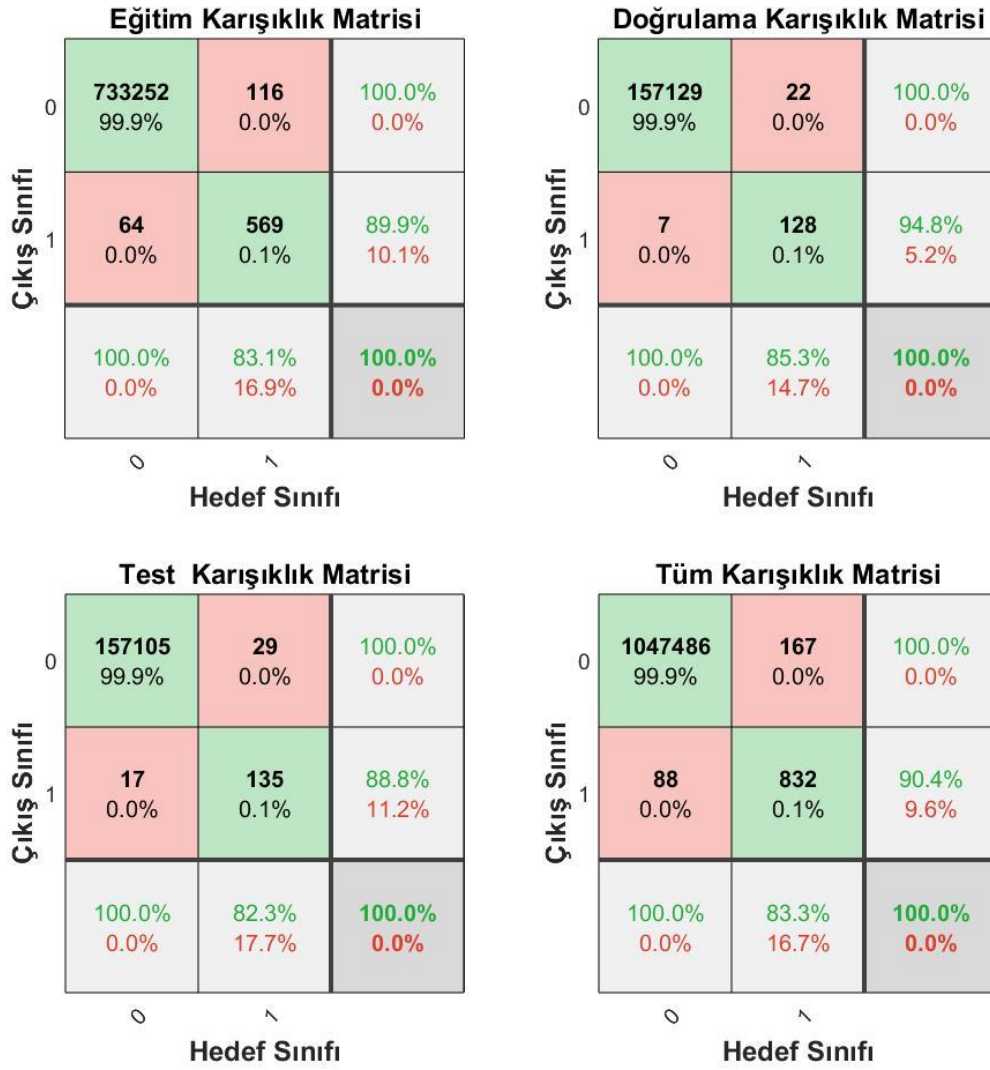
Şekil 4.14. DoS saldırısı ait doğruluk ve karışıklık matrisi (0: DoS Saldırı Değil, 1: DoS Saldırısı).



Şekil 4.15. Probe saldırısı ait doğruluk ve karışıklık matrisi (0: Probe Saldırı Değil, 1: Probe Saldırısı).



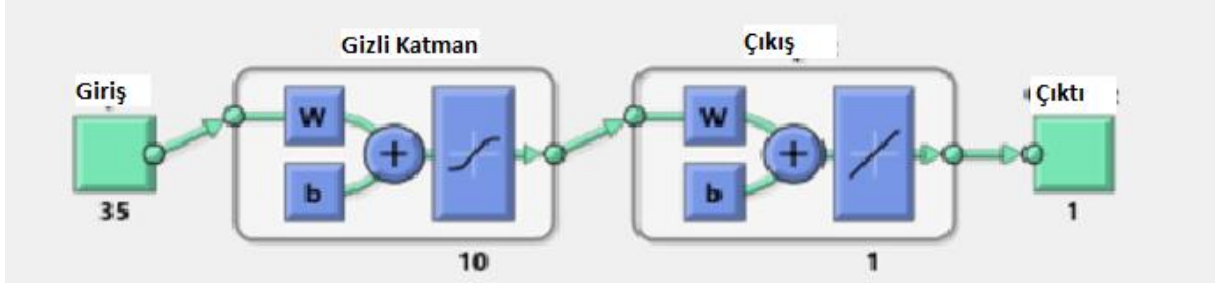
Şekil 4.16. R2L saldırısı ait doğruluk ve karışıklık matrisi (0: R2L Saldırı Değil, 1: R2L Saldırısı).



Şekil 4.17. U2R saldırısı ait doğruluk ve karışıklık matrisi (0: U2R Saldırı Değil, 1: U2R Saldırısı).

Tablo 4.4'deki verilen değerler ölçülürken aşağıdaki yöntem uygulanmıştır.

Modeldeki giriş parametreleri sabit bırakılmıştır. Eğitim, Doğrulama ve Test veri setindeki örneklem sayıları da aynı olacak şekilde modelleme yapılmıştır. 10 Gizli Katmanlı modelin yapısı aşağıdaki gibidir.



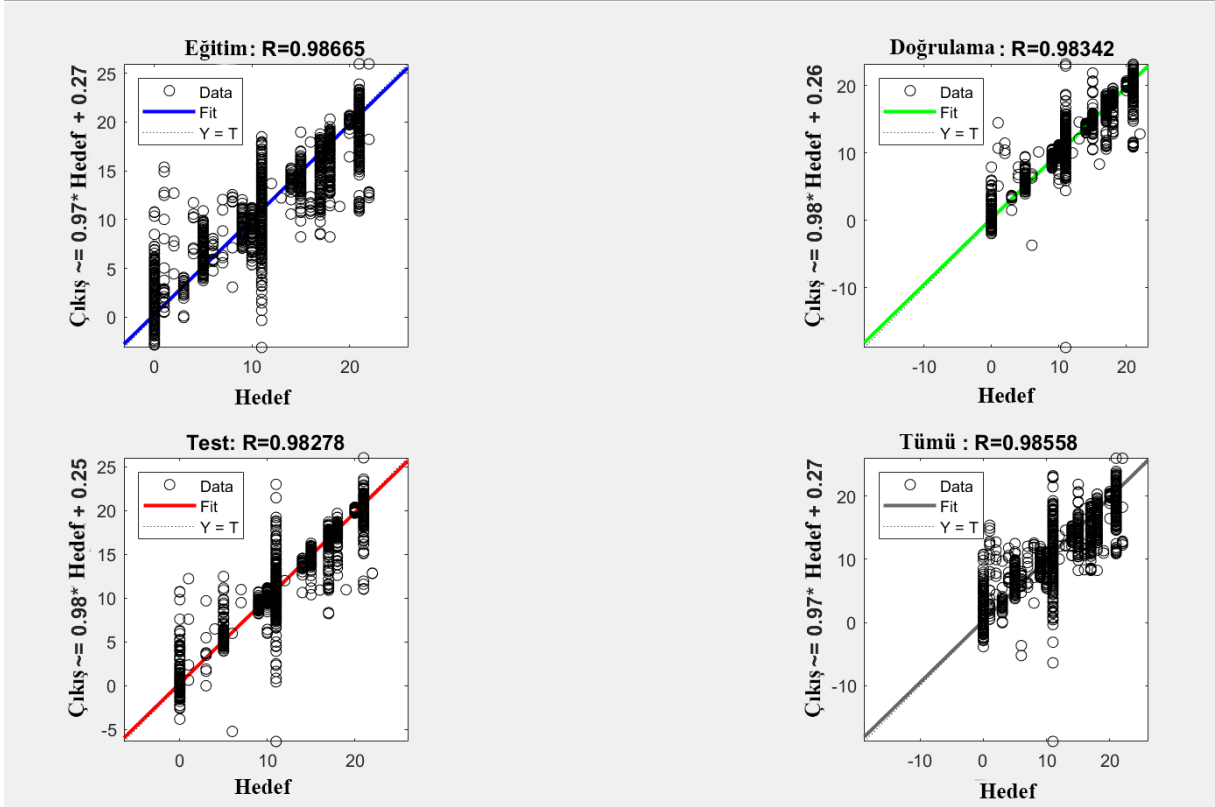
Şekil 4.18. 10 Gizli Katmanlı YSA Modeli.

10 gizli katmanlı modelleme neticesinde aşağıdaki sonuçlara ulaşılmıştır.

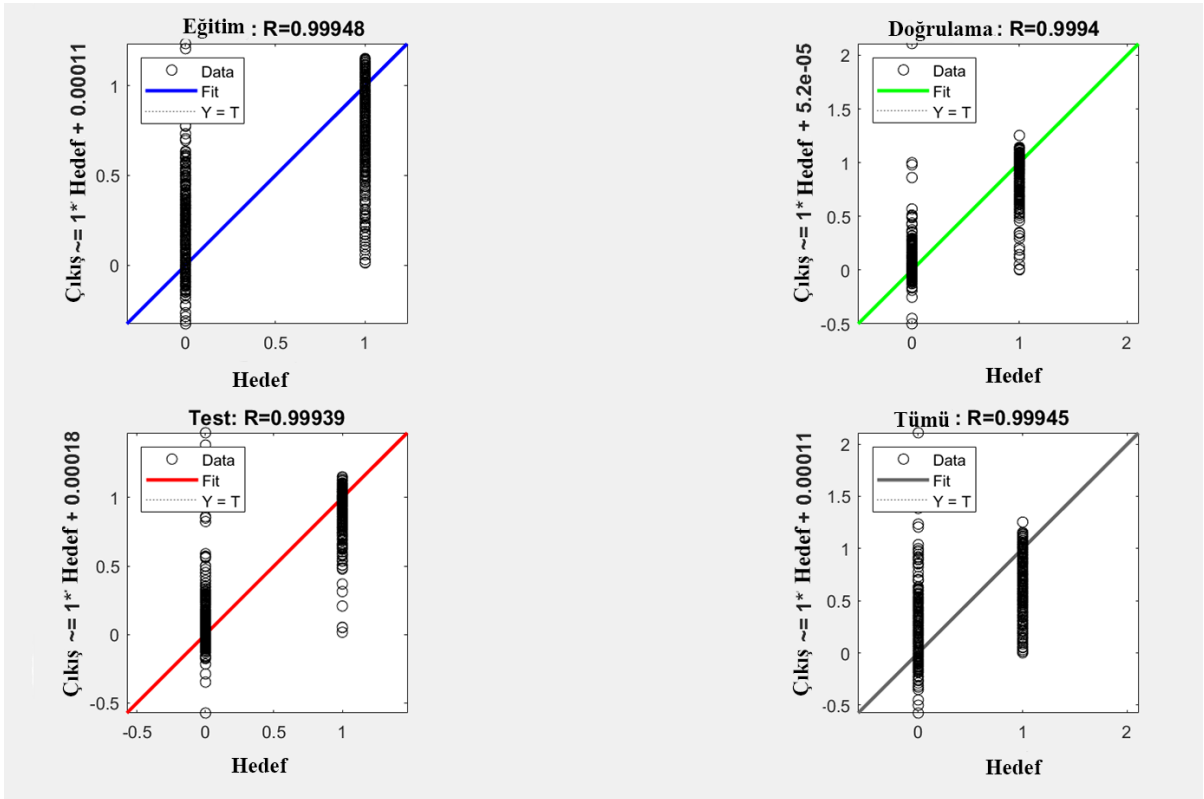
- Training veri seti üzerinde en başarılı sonuçlar DoS saldırılarının çıktı olan modelde elde edilmiş ve bu oran 0,9997'dir.
- Validation veri seti üzerinde en başarılı sonuçlar 0,9996'lık oranla DoS saldırılarının tahmin etmede elde edilmiştir.
- Modelin test edilmesinde kullanılan Test veri setindeki tahminde ise en başarılı sonuçlar Saldırı Türü'nün çıktı olduğu modelde elde edilmiştir.
- Yukardaki tablodaki veriler göz önünde bulundurulduğunda Saldırı Türü (Satan, Neptune, ftp write vb.), Saldırı (Saldırı olup olmadığı), Saldırı Üst Türü (DoS, Probe, U2R ve R2L), DoS (DoS saldırısı olup olmadığı) ve Probe (Probe saldırısı olup olmadığı) saldırıların modelin %100'e yakın bir doğruluk oranı olduğu görülmektedir.
- R2L (R2L saldırısı olup olmadığı) ve U2R (U2R saldırısı olup olmadığı) modelin eğitilmesindeki örneklem sayısının az olması (R2L =52, U2R=1000) nedeni ile başarı oranı düşük çıkmıştır.

Tablo 4.5. 30 Gizli Katmanlı ve Farklı Çıkış Parametresine Göre Sonuçlar.

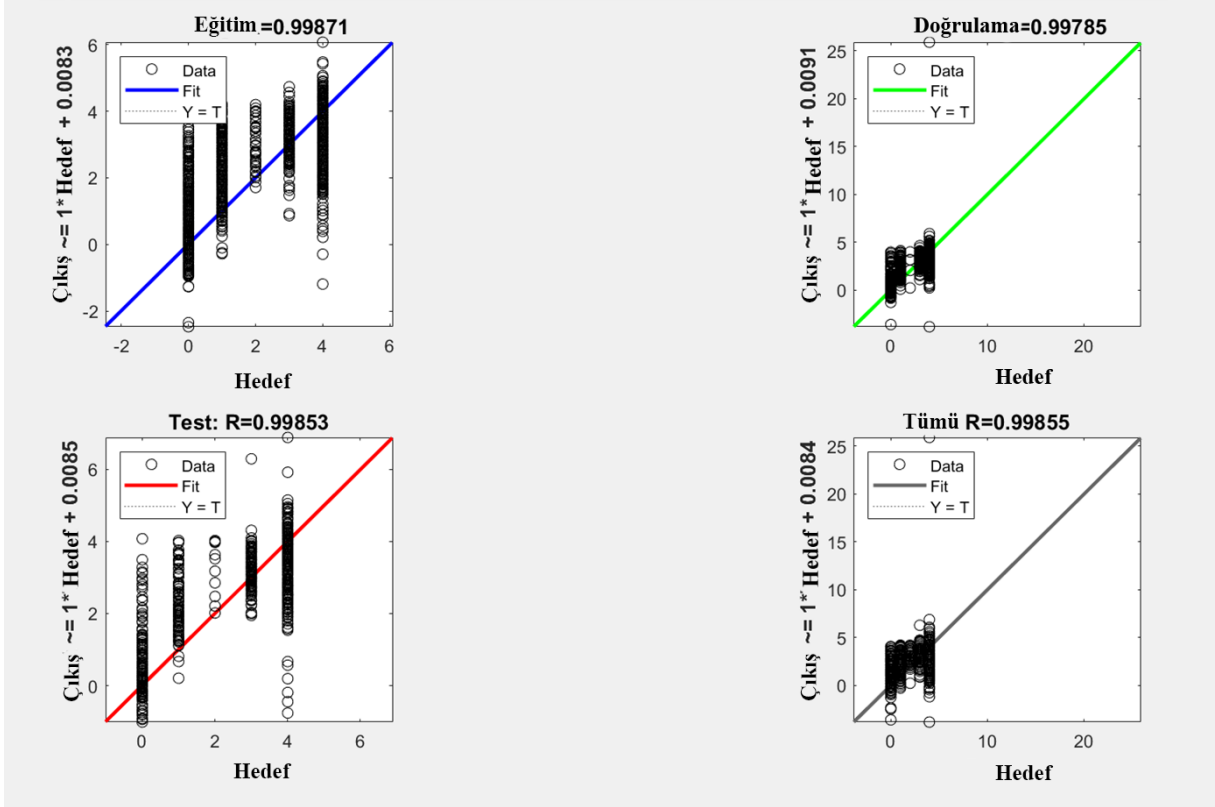
30 Gizli Katmanlı ve Farklı Çıkış Parametresine Göre Sonuçlar							
	Saldırı Türü	Saldırı	Üst Saldırı Türü	Dos	Probe	R2L	U2R
Giriş Parametre Adeti	35						
Hidden Layer	30						
Öğrenme Algoritması	Levenberg-Marquard						
Epoch	109	75	51	138	157	26	54
Süre	00:21:00	00:17:45	00:11:18	00:32:12	00:36:24	00:05:51	00:11:27
Eğitim Seti Örnek Sayısı	734001						
Doğrulama Seti Örnek Sayısı	157286						
Test Seti Örnek Sayısı	157286						
Eğitim MSE	0,04002	0,000187	0,007416	0,000089	0,000159	0,000026	0,000195
Doğrulama MSE	0,04989	0,000215	0,012315	0,000134	0,000259	0,000034	0,00018
Test MSE	0,05128	0,000221	0,008446	0,000226	0,000213	0,000062	0,000225
Eğitim R	0,9866	0,9995	0,9987	0,9998	0,9939	0,5824	0,8946
Doğrulama R	0,9834	0,9994	0,9978	0,9996	0,9899	0,6406	0,8891
Test R	0,9827	0,9994	0,9985	0,9994	0,9921	0,5613	0,8709



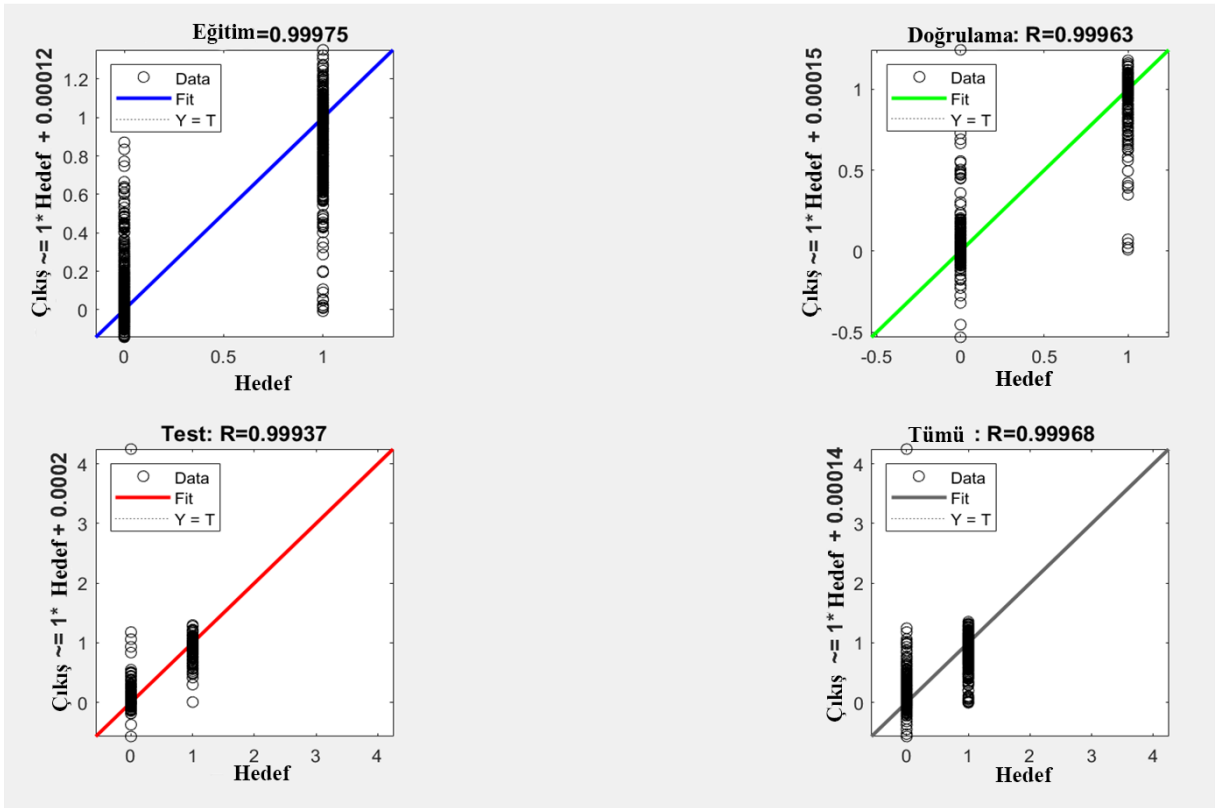
Şekil 4.19. Saldırı çıktısına ait plot regresyon grafiği (satan, neptune, vb).



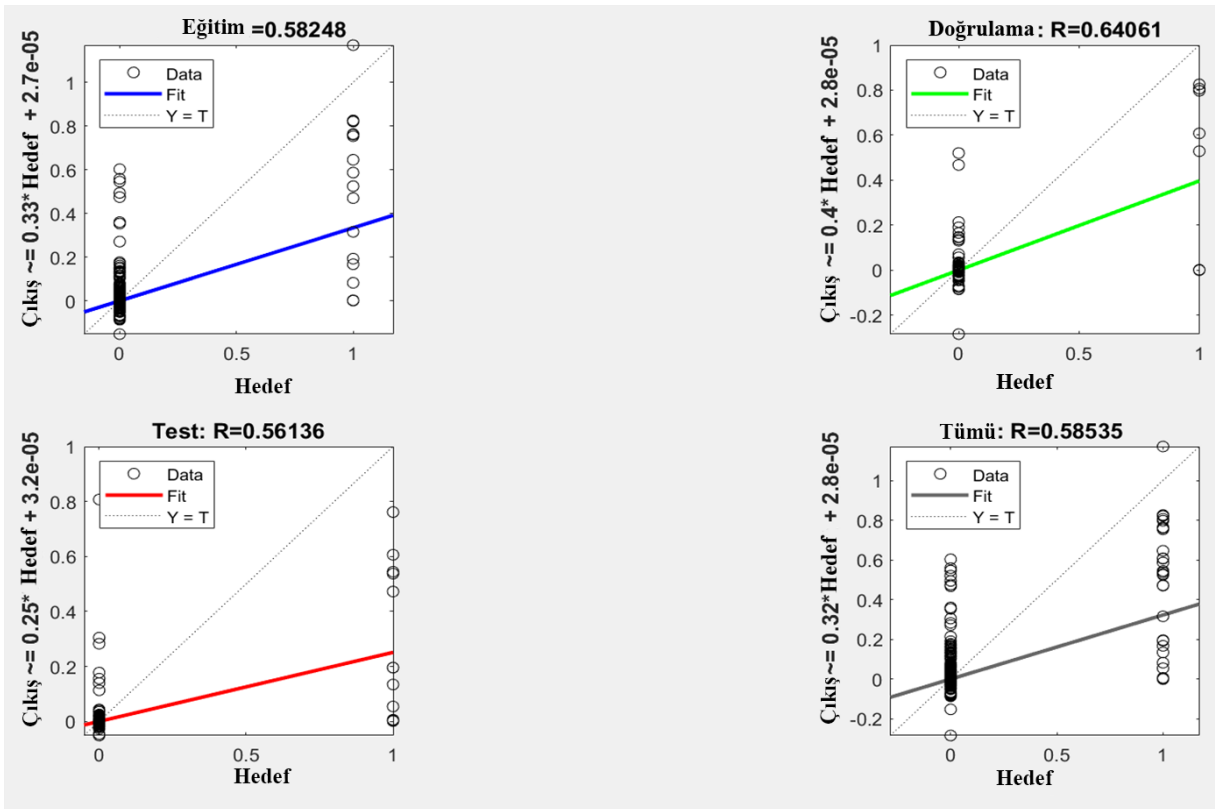
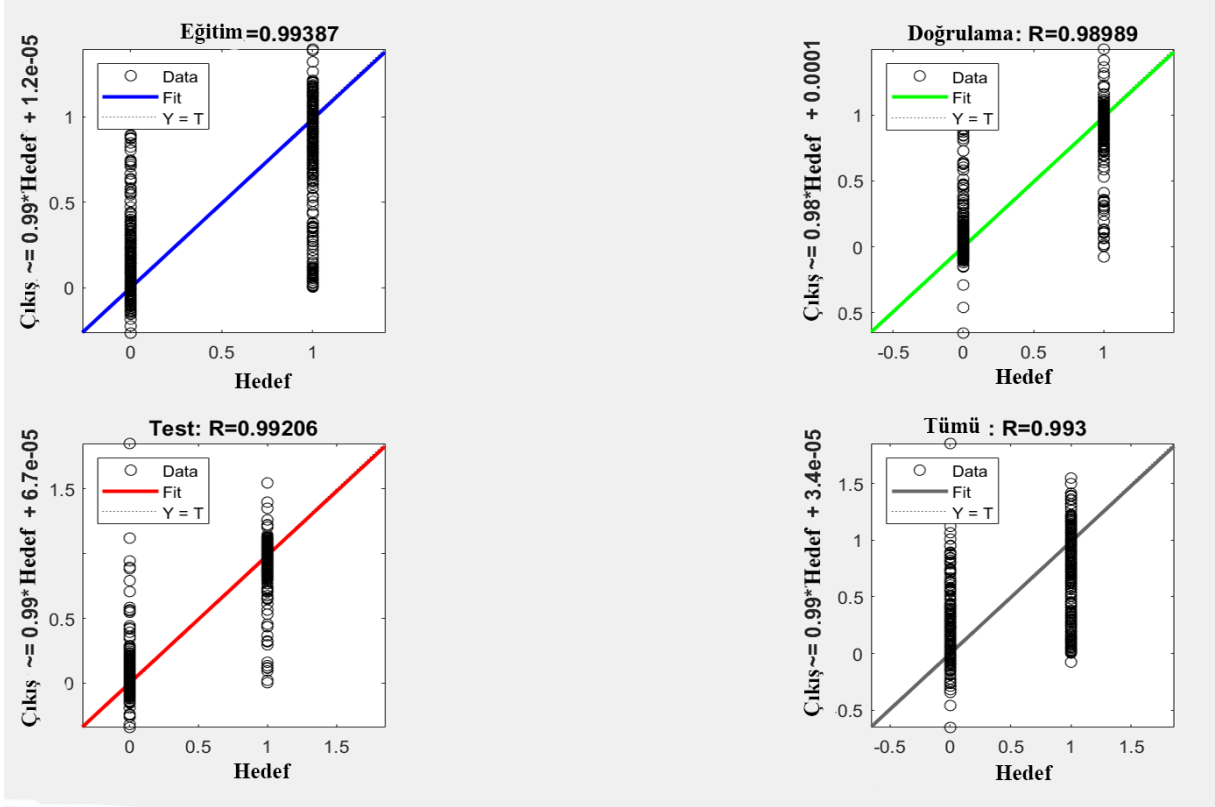
Şekil 4.20. Saldırı olup olmadığına ait plot regresyon grafiği (Evet, Hayır).

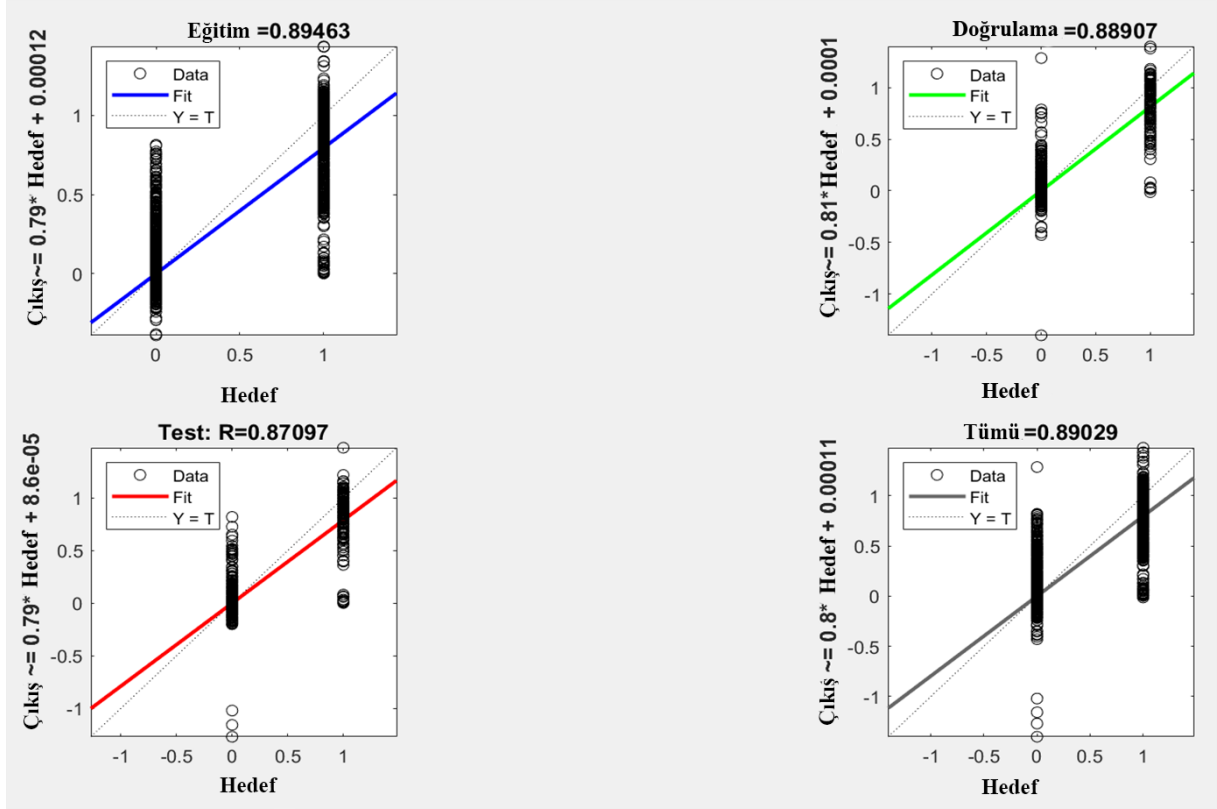


Şekil 4.21. Saldırı tipine ait plot regresyon grafiği (DoS, Probe, U2R ve R2L).



Şekil 4.22. DoS saldırısı Olup Olmadığına ait plot regresyon grafiği (Evet, Hayır).

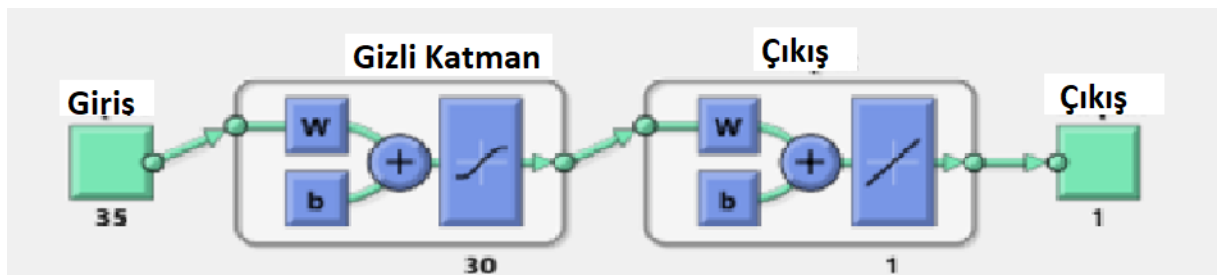




Şekil 4.25. U2R saldırısı olup olmadığına ait plot regresyon grafiği (Evet, Hayır).

Tablo 4.5’deki verilen değerler ölçülürken aşağıdaki yöntem uygulanmıştır.

Modeldeki giriş parametreleri sabit bırakılmıştır. Eğitim, Doğrulama ve Test veri setindeki örneklem sayıları da aynı olacak şekilde modelleme yapılmıştır. 30 Gizli Katmanlı modelin yapısı aşağıdaki gibidir.



Şekil 4.26 30 Gizli Katmanlı YSA Modeli.

30 gizli katmanlı modelleme neticesinde aşağıdaki sonuçlara ulaşılmıştır.

- Training veri seti üzerinde en başarılı sonuçlar DoS saldırılarının çıktı olan modelde elde edilmiş ve bu oran 0.9998’dir.
- Validation veri seti üzerinde en başarılı sonuçlar 0,9996’lık oranla DoS saldırılarının tahmin etmede elde edilmiştir.

- Modelin test edilmesinde kullanılan Test veri setindeki tahminde ise en başarılı sonuçlar Saldırı ve DoS çıktı olduğu modelde elde edilmiştir.
- Yukardaki tabloda belirtilen veriler göz önünde bulundurulduğunda Saldırı Türü (Satan, Neptune, ftp write vb.), Saldırı (Saldırı olup olmadığı), Saldırı Üst Türü (DoS, Probe, U2R ve R2L), DoS (DoS saldırısı olup olmadığı) ve Probe (Probe saldırısı olup olmadığı) saldırıların modelin %99'un üzerinde doğruluk oranı olduğu görülmektedir.
- R2L (R2L saldırısı olup olmadığı) ve U2R (U2R saldırısı olup olmadığı) modelin eğitilmesindeki örneklem sayısının az olması (R2L =52, U2R=1000) nedeni ile başarı oranı düşük çıkmıştır.

10 ve 30 gizli katmanlı YSA modeli birlikte değerlendirildiğinde aşağıdaki sonuçlar ortaya çıkmaktadır.

1. 10 gizli katmanlı modelin başarısı 30 katmanlı modele göre daha iyidir.
2. 30 gizli katmanlı modelin eğitilmesi 10 gizli katmanlı modele göre daha çok zaman almaktadır.
3. Her iki modelde en başarılı sonuçlar DoS saldırısını tahmin etmede elde edilmiştir.
4. Her iki modelde doğruluk oranı en düşük sonuçlar R2L saldırı türündedir.
5. Bazı özelliklerin modelden çıkarılıp modelin eğitilmesi neticesinde elde edilen sonuçların başarı oranı düşmektedir. Buna karşın modelin karmaşıklığı ve sistem kaynağı ihtiyacı düşmektedir.

Tablo 4.6. Decision Trees algoritması test sonuçları.

Parametre Sayısı	Öğrenme Modeli	Tür	Alt Model	Eğitim Süresi	Doğruluk Oranı
35	Classification Learner	Saldırı	Fine Tree	102.39 Saniye	100%
			Medium Tree	56.202 Saniye	99,80%
			Coarse Tree	41.966 Saniye	99,50%
		Saldırı Üst Sınıf	Fine Tree	47,67 Saniye	100%
			Medium Tree	51,111 Saniye	100%
			Coarse Tree	46,354 Saniye	99,90%
		DoS	Fine Tree	96,727 Saniye	100%
			Medium Tree	48,226 Saniye	99,80%
			Coarse Tree	36,06 Saniye	99,50%
		R2L	Fine Tree	55,475 Saniye	100%
			Medium Tree	51,222 Saniye	100%
			Coarse Tree	34,961 Saniye	100%
		Probe	Fine Tree	84,222 Saniye	100%
			Medium Tree	47,647 Saniye	99,90%
			Coarse Tree	37,919 Saniye	99,30%
		U2R	Fine Tree	100,77 Saniye	100%
			Medium Tree	68,056 Saniye	100%
			Coarse Tree	38,395 Saniye	99,90%
		Saldırı Tipi	Fine Tree	70,851 Saniye	99,80%
			Medium Tree	48,414 Saniye	99,30%
			Coarse Tree	40,453 Saniye	98,20%

Yukardaki veriler ışığında aşağıdaki sonuçlar elde edilmiştir.

Algoritmanın doğruluğu (Accuracy) aşağıdaki şekilde hesaplanmaktadır.

True Positive – TP = Gerçekte saldırı olan ve tahminde saldırı olarak tahmin edilen.

True Negative – TN =Gerçekte saldırı olmayan ve tahminde saldırı değil olarak tahmin edilen.

Doğruluk Oranı=100 * (($\sum$ TP + $\sum$ TN) / Toplam Örneklem)

Gerçekte saldırı olan ve tahminde saldırı olarak tahmin edilen:

True Positive – TP = 246925

Gerçekte saldırı olmayan ve tahminde saldırı değil olarak tahmin edilen:

True Negative – TN = 801581

Gerçekte saldırı olan ve tahminde saldırı değil olarak tahmin edilen:

False Positive – FP = 30

Gerçekte saldırı olmayan ve tahminde saldırı olarak tahmin edilen:

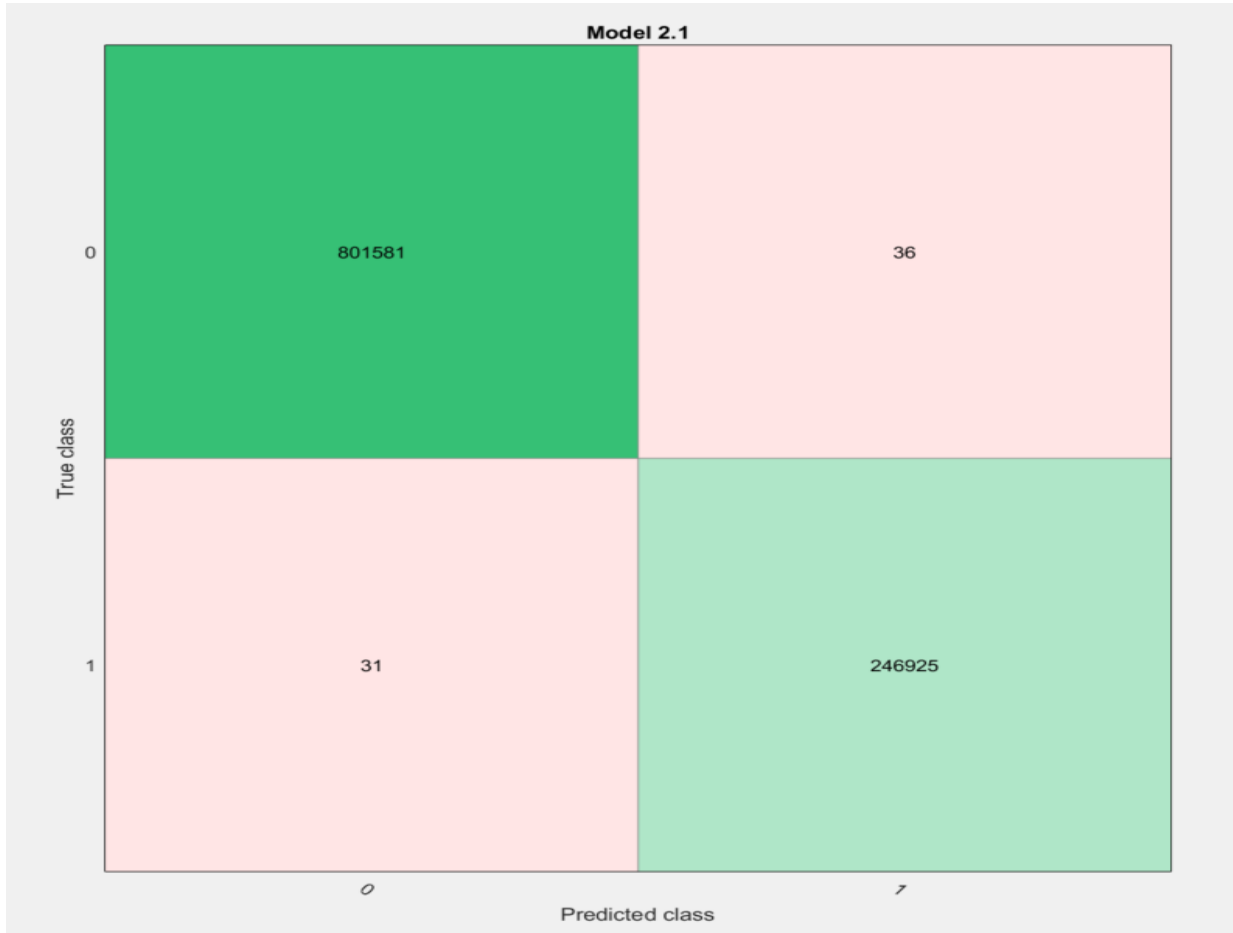
False Negative – FN = 31

Doğruluk Yüzdesi = $100 * (TN + TP / TOPLAM) \Rightarrow 100 * (1.048.506 / 1.048.567)$
 $= 99,99419 \cong 100$

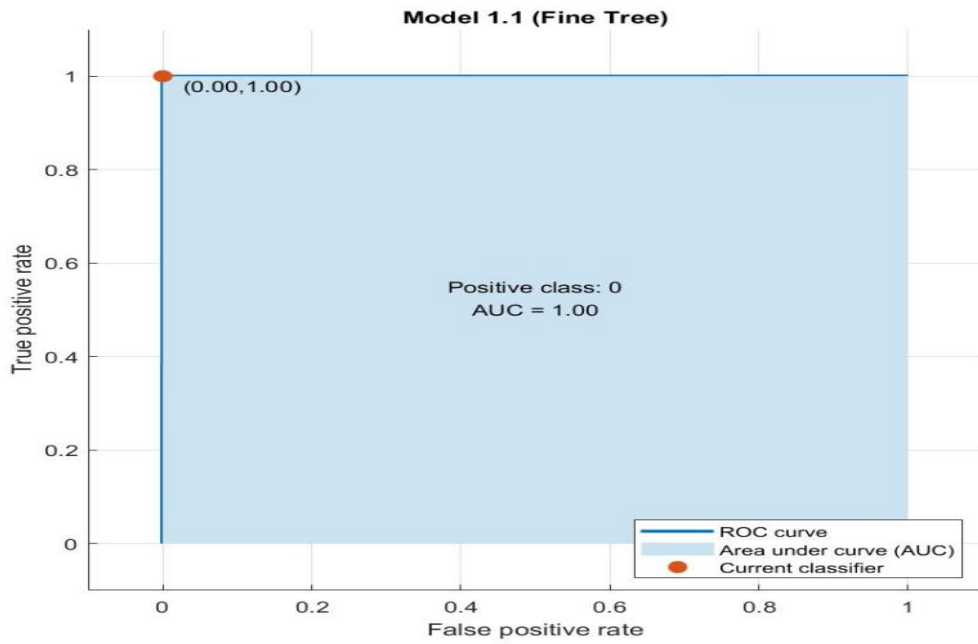
Bağlantının saldırı olup olmadığı ile ilgili en iyi sonuç Fine Tree algoritması ile ve %100 lük doğruluk oranı ile elde edilmiştir.

Yukarda, bağlantının saldırı olup olmadığı ile ilgili sonuçlar üzerinde doğruluk oranı hesaplanmıştır. Bu işlem diğer değerler için de kullanılabilir.

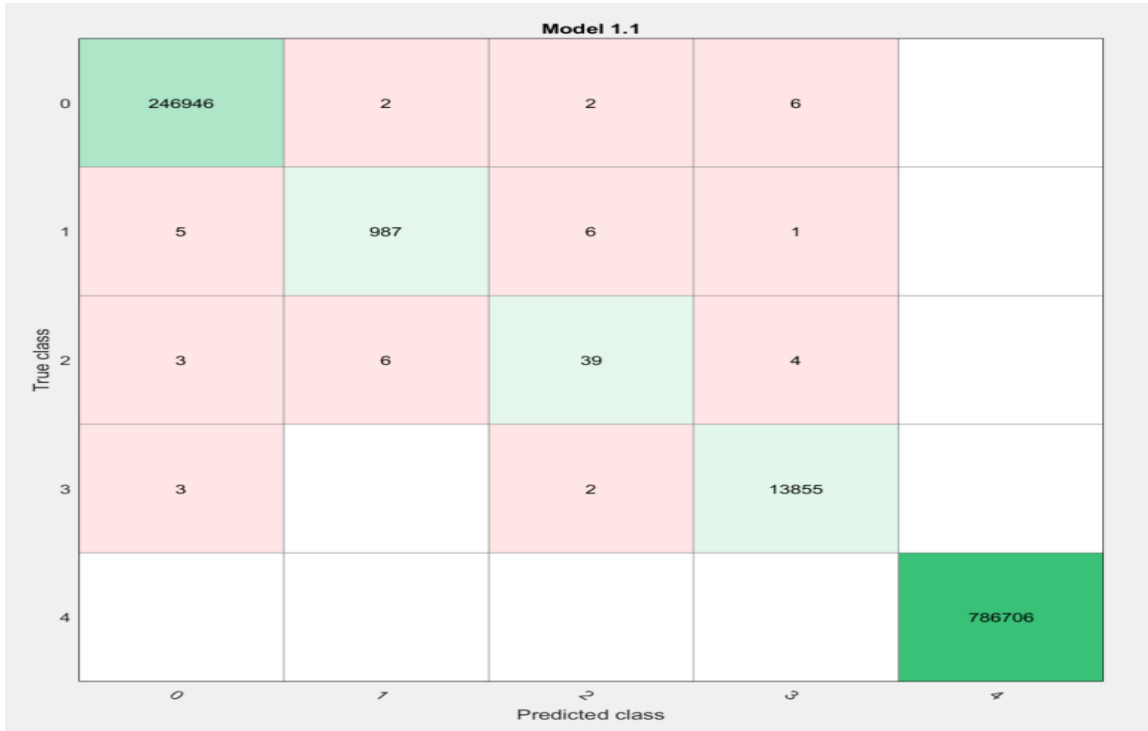
Sonuçlara ait Hata Matrisi ROC eğrisi aşağıdaki gibidir:



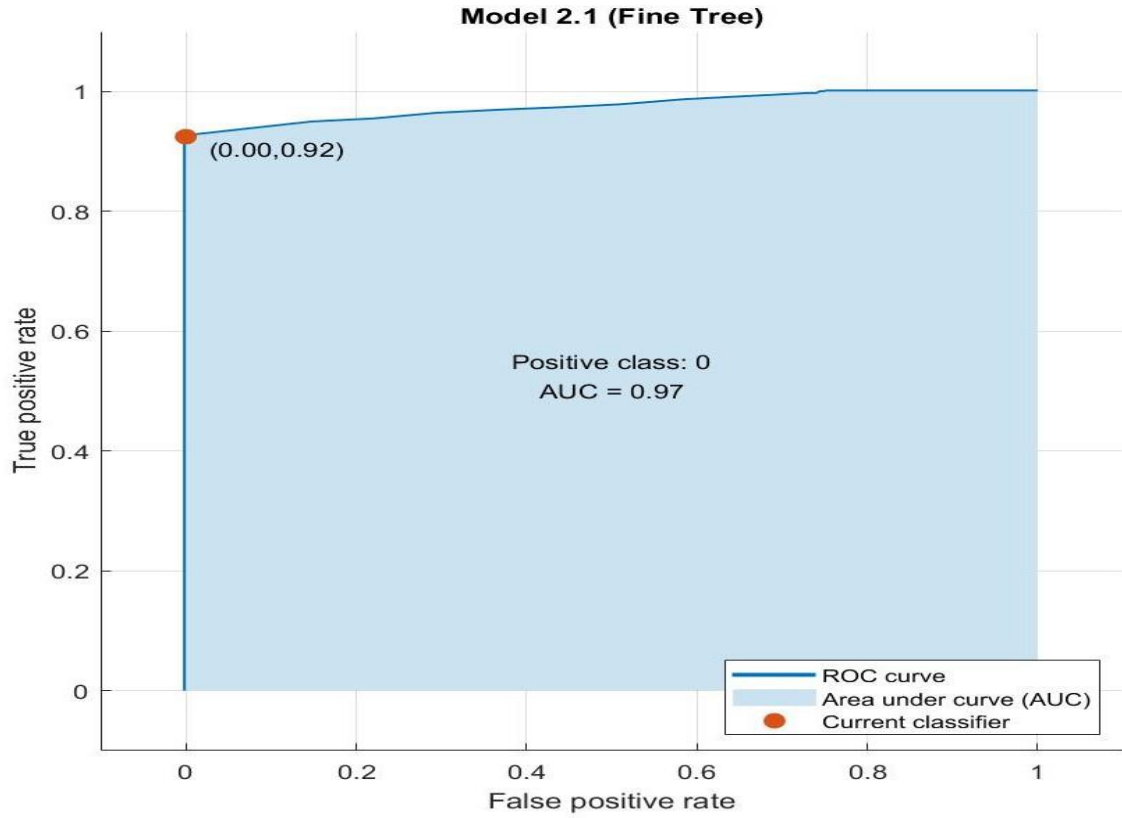
Şekil 4.27. Saldırı çıktı değerine ait hata matrisi (1=Evet, 0=Hayır).



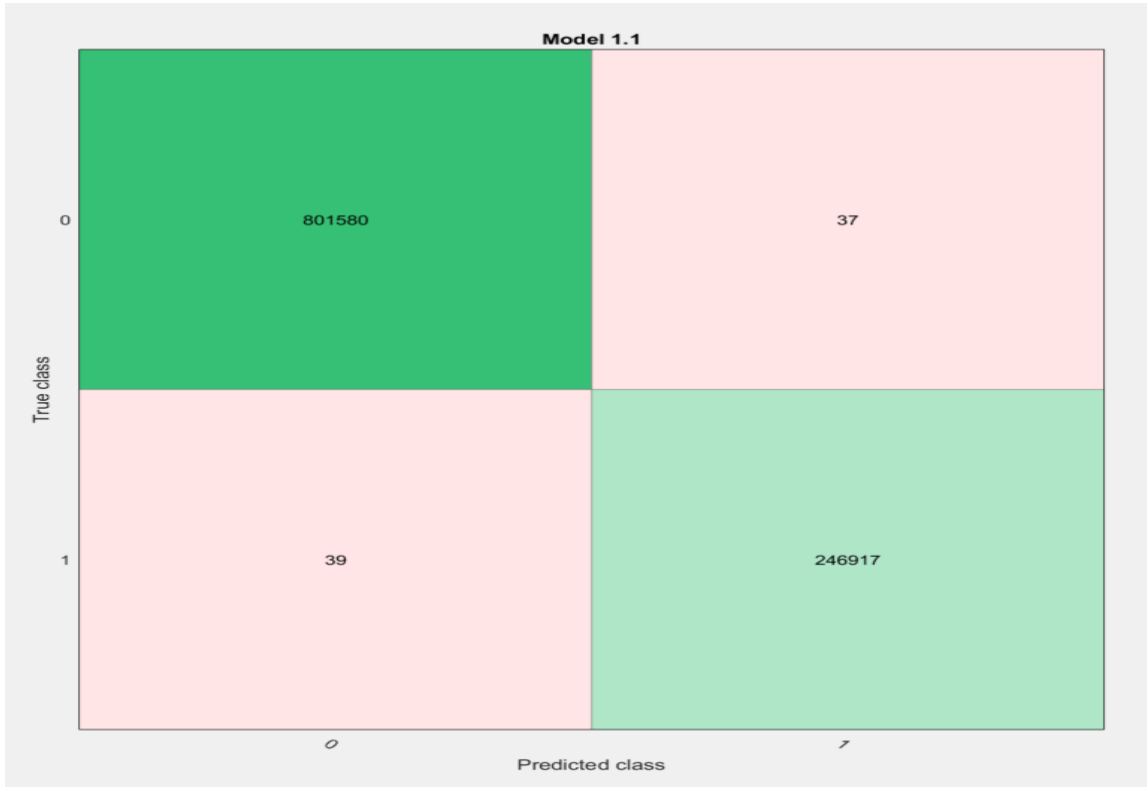
Şekil 4.28. Saldırı çıktı değerine ait ROC Eğrisi.



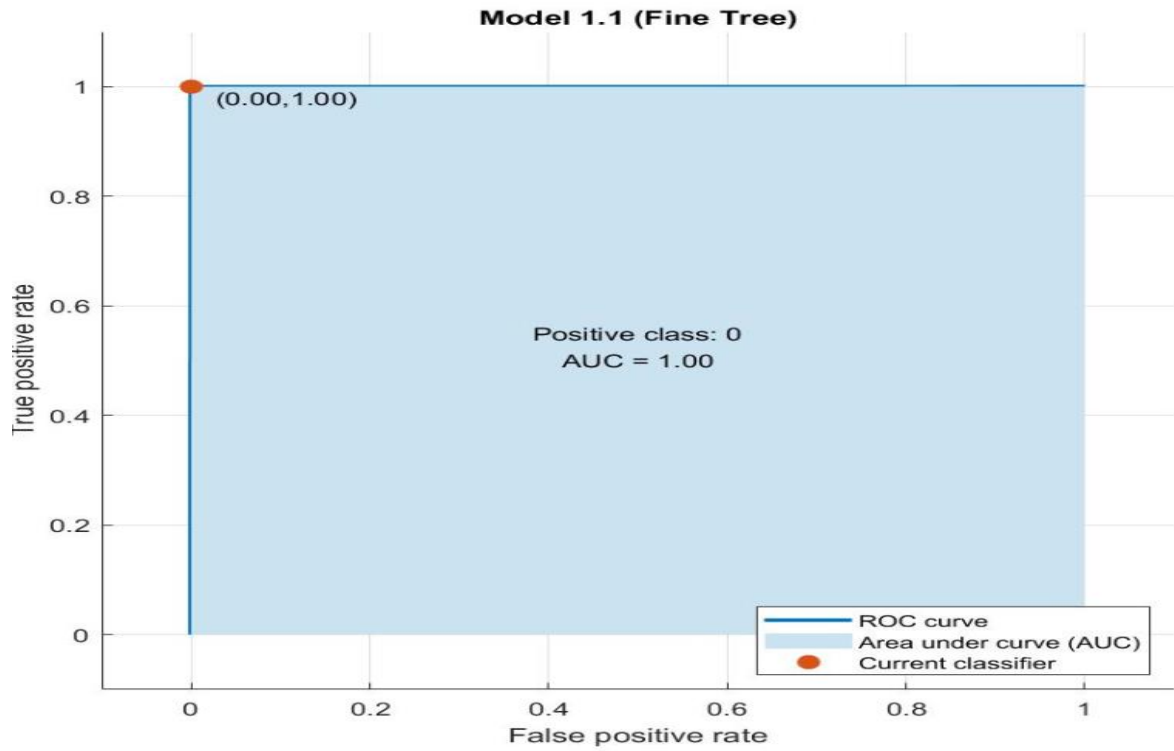
Şekil 4.29. Saldırı Üst Türüne ait hata matrisi (Dos, Probe vb.).



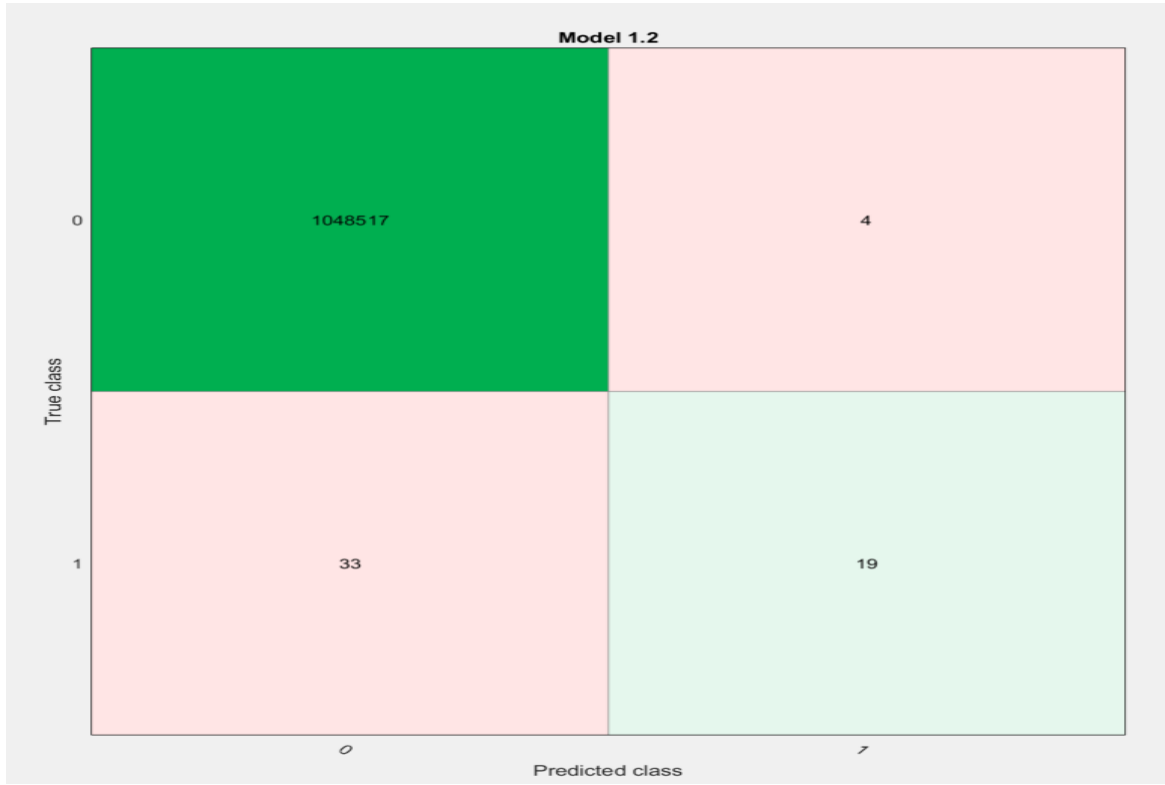
Şekil 4.30. Saldırı Üst Sınıf saldırı türüne (DoS, U2R, R2L, Probe) ait ROC Eğrisi.



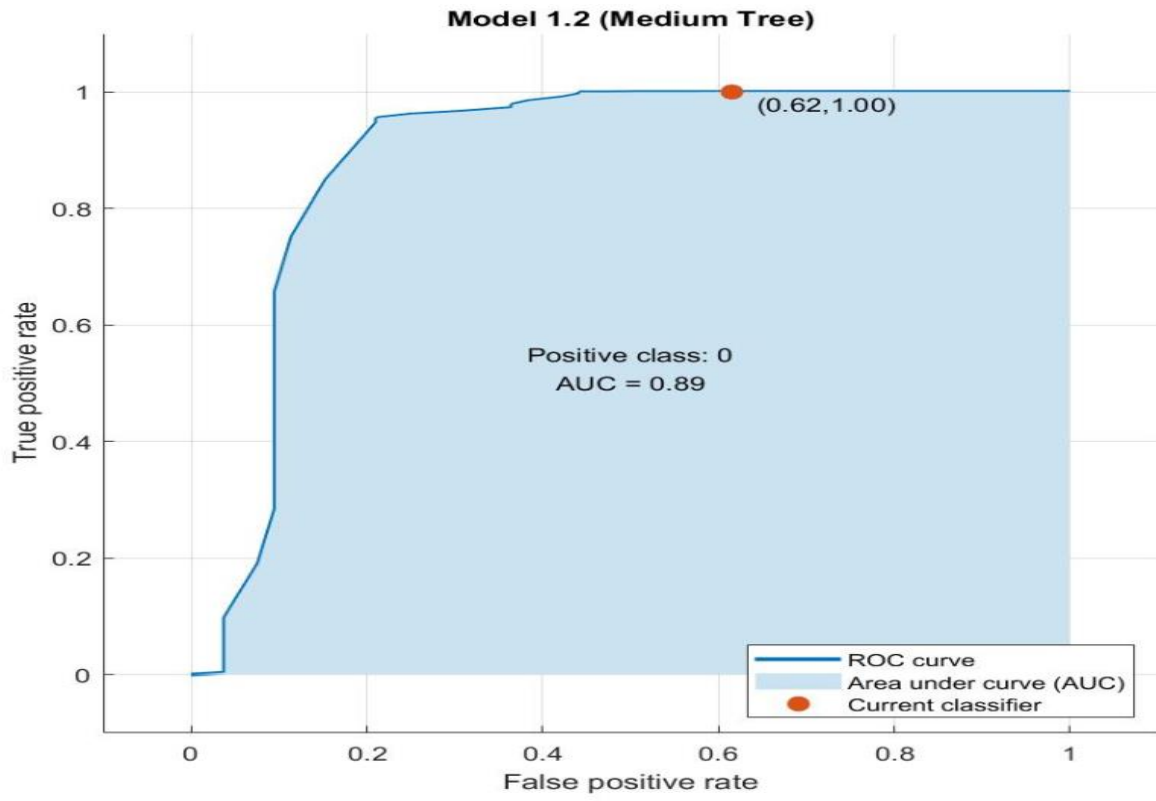
Şekil 4.31. DoS Saldırısına ait hata matrisi (1=Evet, 0=Hayır).



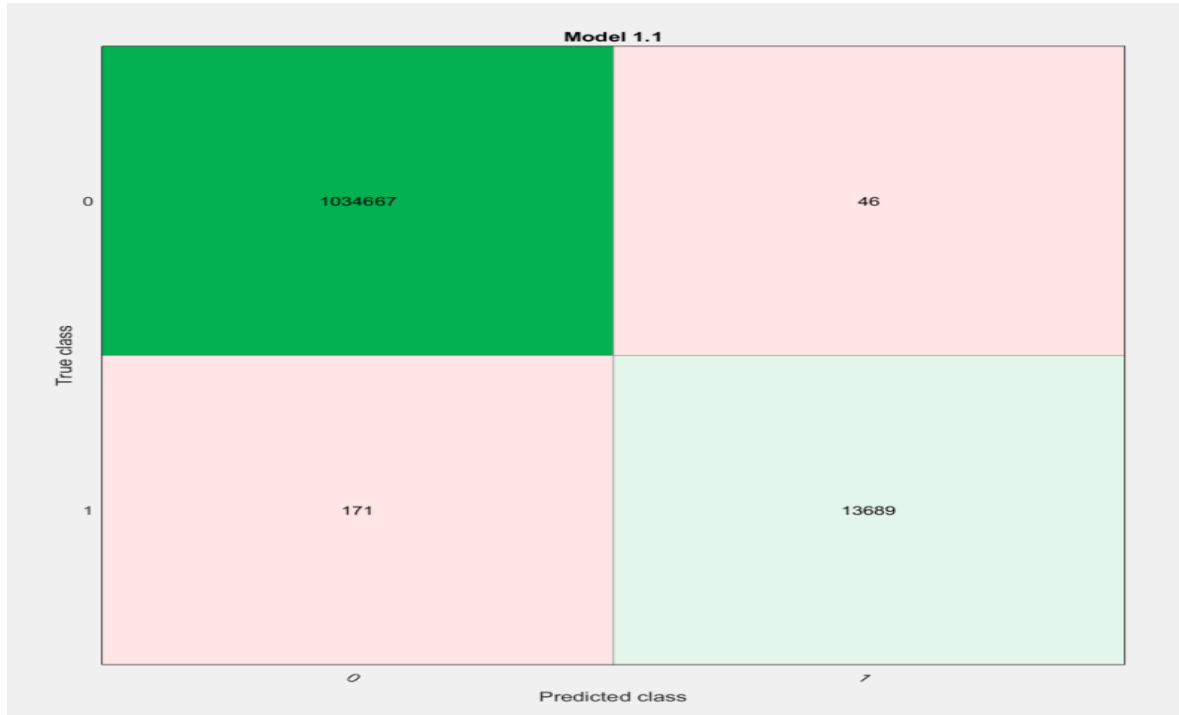
Şekil 4.32. DoS saldırı türüne ait ROC Eğrisi



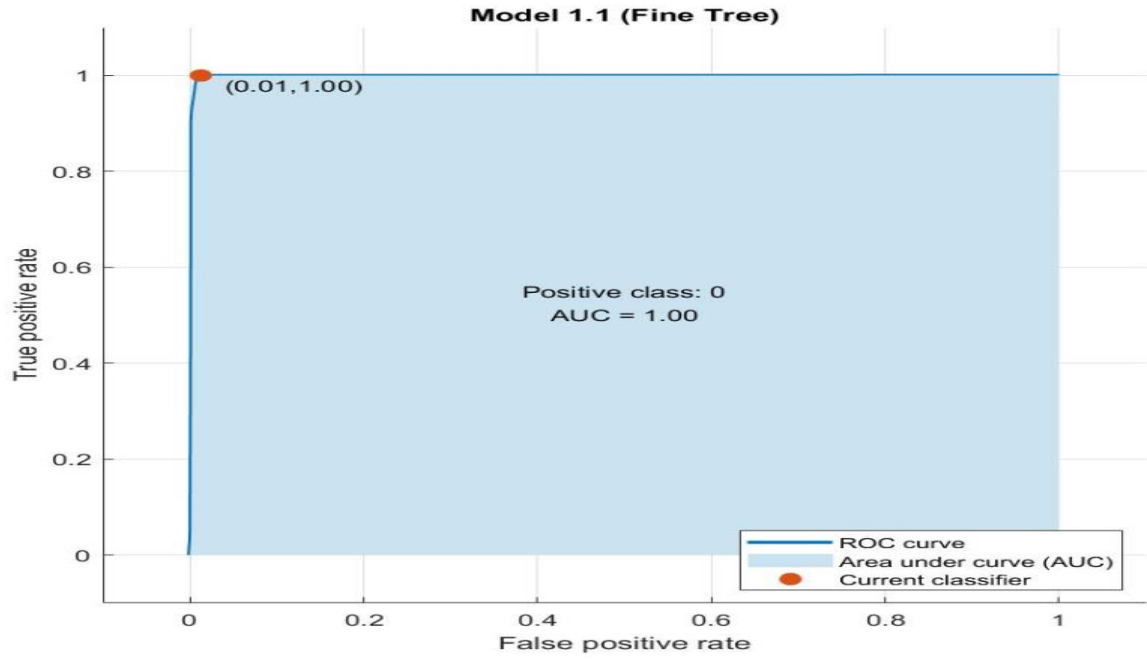
Şekil 4.33. R2L Saldırısına ait hata matrisi (1=Evet, 0=Hayır).



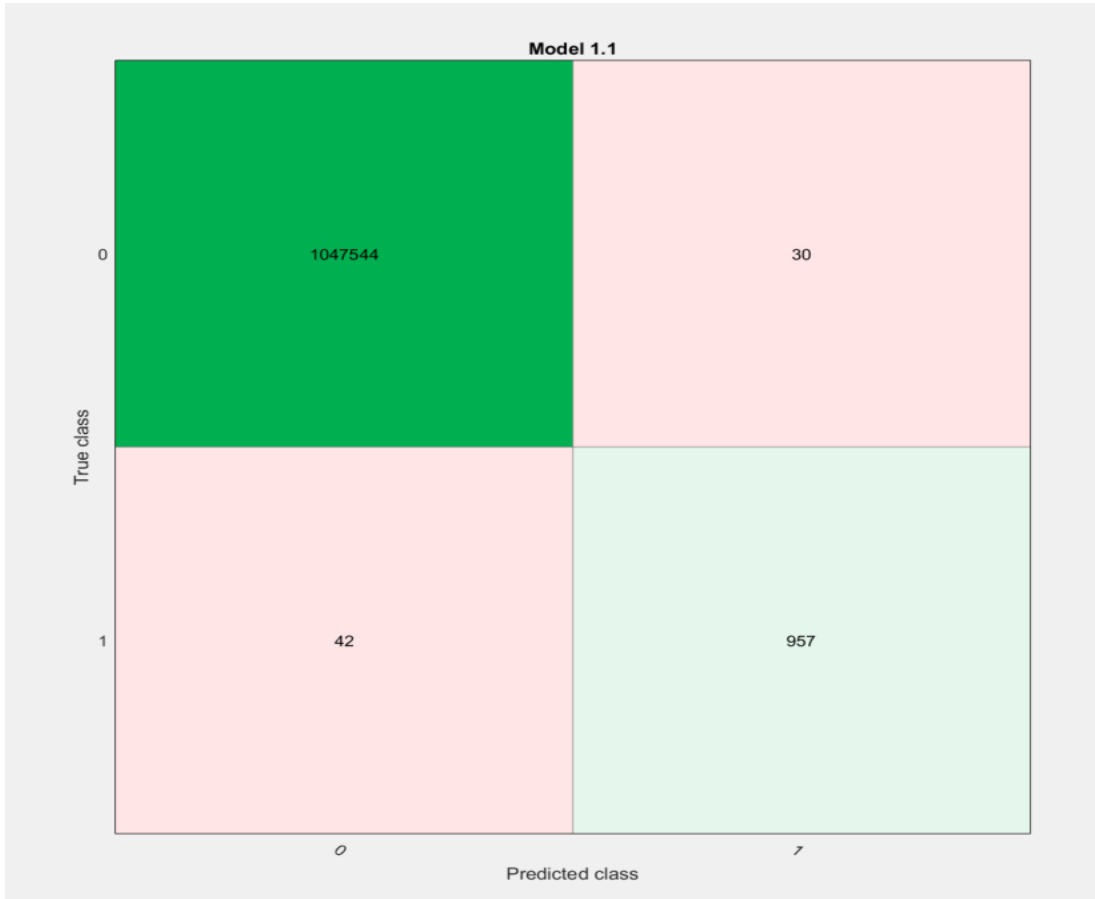
Şekil 4.34. R2L Saldırı türüne ait ROC eğrisi.



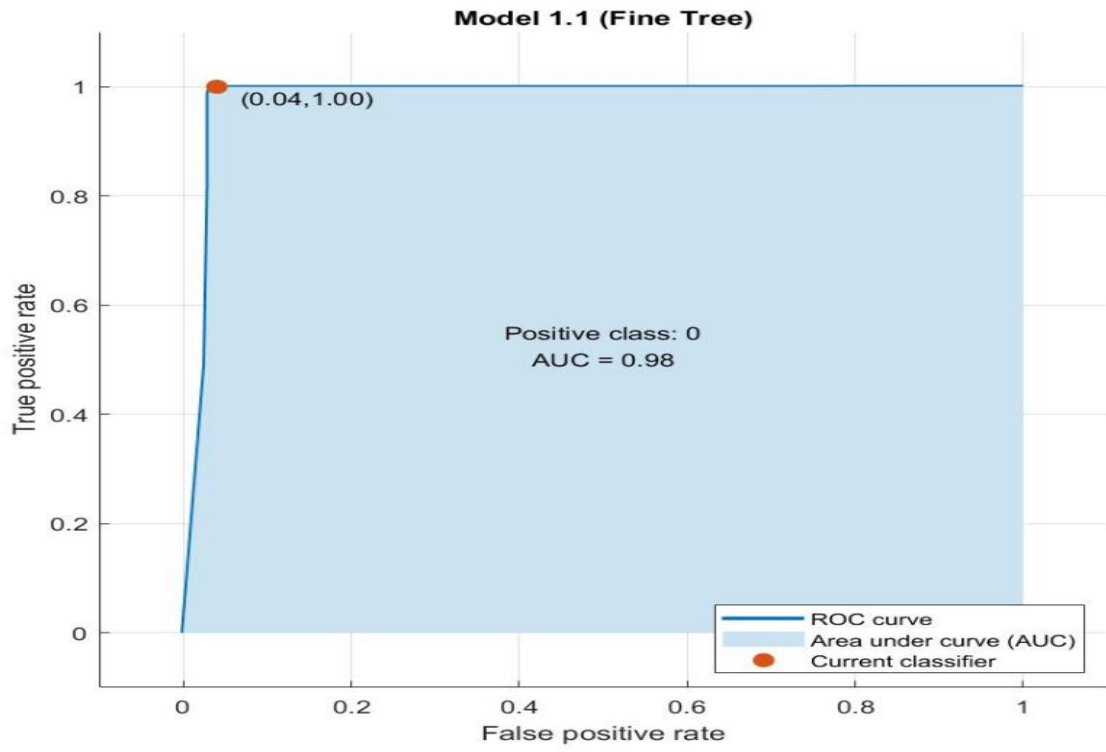
Şekil 4.35. Probe Saldırısına ait hata matrisi (1=Evet, 0=Hayır).



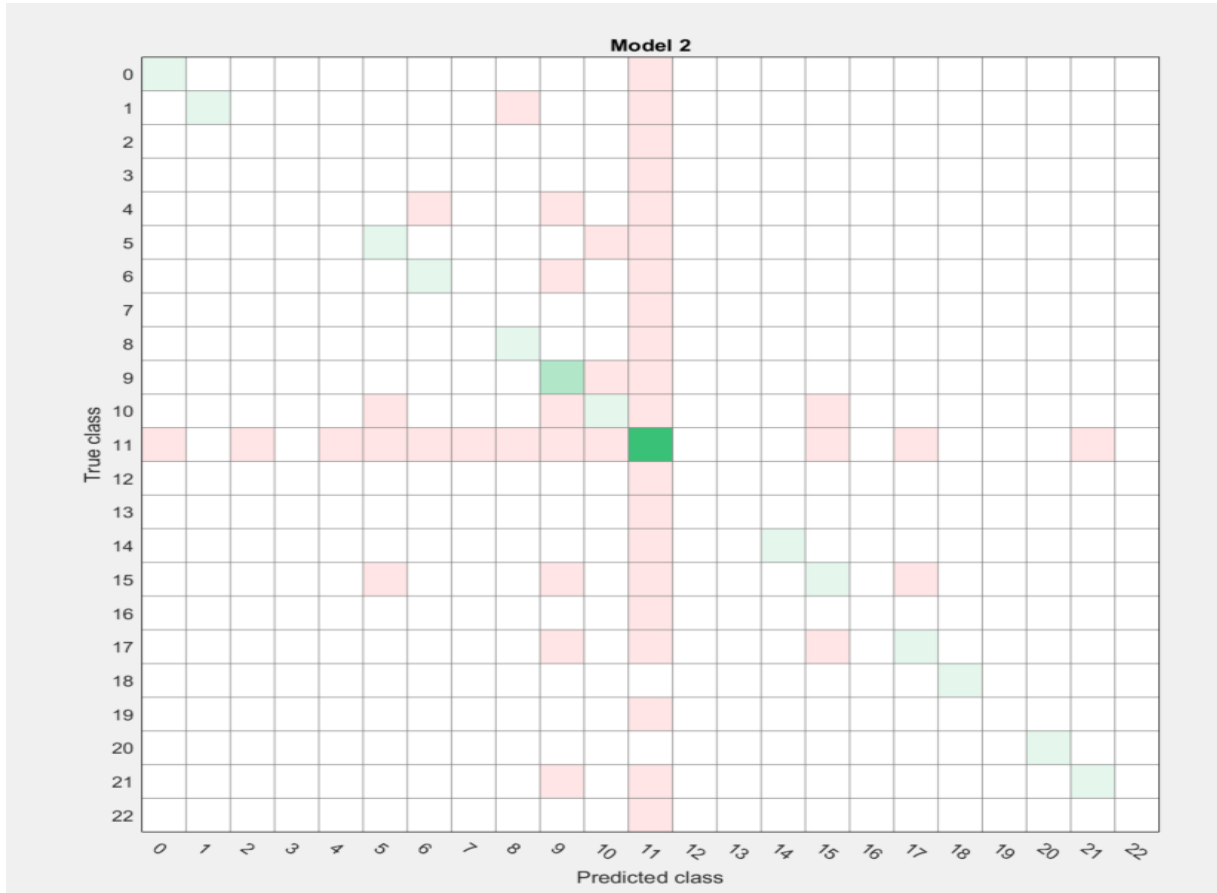
Şekil 4.36. Probe saldırı türüne ait ROC eğrisi.



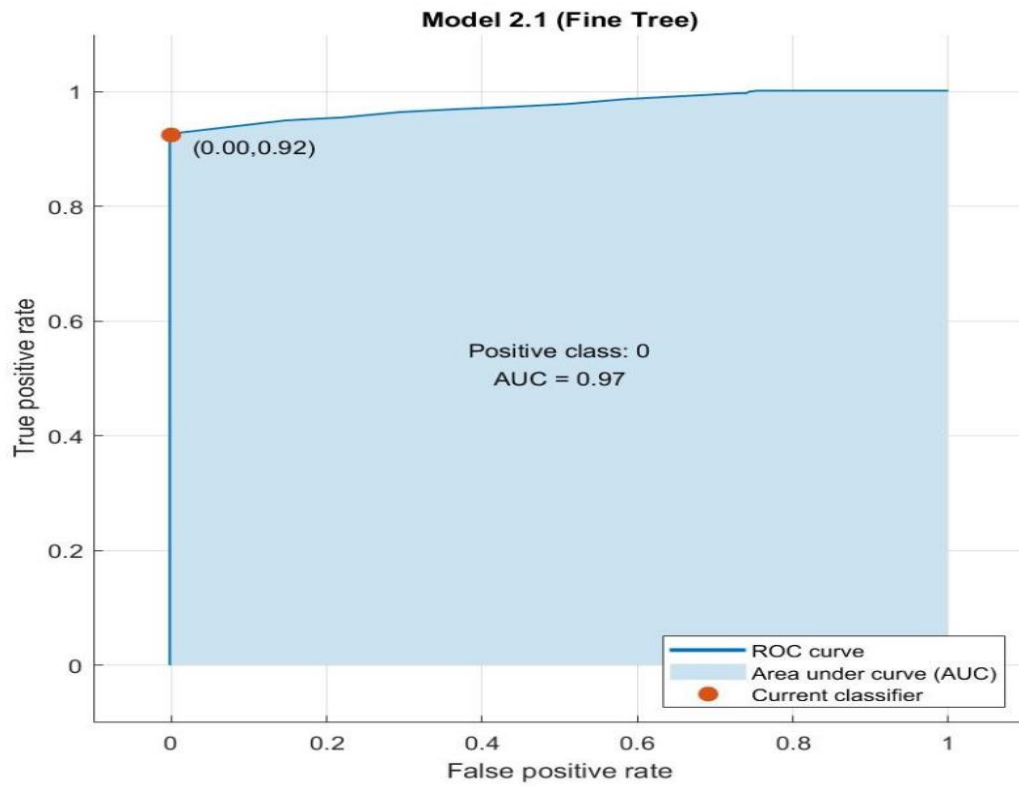
Şekil 4.37. U2R Saldırısına ait hata matrisi (1=Evet, 0=Hayır).



Şekil 4.38. U2R Saldırı türüne ait ROC eğrisi.



Şekil 4.39. Saldırı çeşidine ait hata matrisi (satan, neptune, vb.).



Şekil 4.40. Saldırı Çeşidine (Satan, neptune, vb.) ait ROC eğrisi.

ROC eğrisine ait şekillerde dikkat edilmesi gereken Eğri Altındaki Alan-Area Under Curve (AUC)'dur. Eğri altındaki alan değeri sınıflandırıcının genel kalitesinin bir ölçüsüdür. Eğri Altındaki Alan değerinin yüksek olması, sınıflandırıcı performansını yüksek olduğunu gösterir.

Bağlantının saldırı olup olmadığı ile ilgili tahmindeki en iyi sonuç Fine Tree algoritması ile ve %100 lük doğruluk oranı ile elde edilmiştir.

Saldırı Üst türündeki tahminler Fine Tree ve Medium tree'de %100'lük bir doğruluk oranına sahiptir.

DoS saldırılarını tahmin etmede en başarılı olan %100'lük oranla Fine Tree algoritmasıdır.

R2L ve U2R saldırı türlerinde YSA algoritmasında elde edilen sonuçların aksine bu saldırı türlerinde %100 'lük oranla doğru tahminler yapılmıştır.

Tablo 4.7. Bu çalışmadaki sonuçlar ile farklı yaklaşımların karşılaştırılması.

	DoS	Probe	U2R	R2L
Agarwal ve ark.,2000	96,90%	73,20%	6,60%	10,70%
Jahanbani ve ark., 2012	99,55%	100%	0%	99,98%
Kayacik ve ark., 2007	96,50%	72,80%	22,90%	11,30%
Jeya ve ark., 2012	96,80%	99,00%	99,90%	73,20%
Bu çalışma, YSA 35	100%	98,6%	83,70%	33,33%
Bu çalışma, YSA 41	100%	100%	100%	100%
Bu Çalışma, DT	100%	100%	100%	100%

Yukardaki tabloda görüleceği üzere en iyi tahminler bu çalışmada yer alan ve YSA 41 özellik ile karar ağaçları modellemesi ile elde edilmiştir.

Modelin özellik seçimi modelin başarısı üzerinde etkisi büyüktür. Yukardaki tabloda görülen sonuçlar altı tane özelliğin modele giriş parametresi olarak eklendiği ve eklenmediği durumdaki sonuçlar ortaya konulmuştur. Modele dahil edilen özellikler modelin performansını karmaşıklığını etkilemektedir.

Modelin eğitilmesinde 41 özellik kullanılması durumunda en iyi başarı oranı elde edilmiştir.

YSA'da 35 özellikle yapılan testlerde R2L ve U2R saldırıların tahmini diğer saldırı tiplerini tahmin etmeye kıyasla daha başarısız olduğu görülmektedir.

5. SONUÇLAR VE ÖNERİLER

6.1 Sonuçlar

Ağ güvenliği her geçen gün daha önemli bir hal almaktadır. Siber güvenliğe ayrılan bütçe de bu doğrultuda artmaktadır. Ağ güvenliğini sağlamadaki bileşenlerinden “saldırı tespit sistemleri” için oluşturulmuş olan KDD’99 veri seti, akıllı model tasarlamaya büyük katkı sağlamaktadır. Tez’de MIT Lincoln Laboratuvarında 9 haftalık süreçte elde edilmiş verilerin güncellenmiş hali olan KDD’99 veri seti hakkında istatistiki bilgiler verilmiştir. Bu veri setindeki bazı saldırı türleri güncelliğini yitirmiştir. Ancak, STS için oluşturulmuş diğer veri setlerine göre daha fazla örneklem barındırmaktadır. Bu örneklemelerin %78’ini oluşturan tekrarlı veri temizlenerek veri seti daha etkin hale getirilmiştir. Veri setindeki tüm özellikler kullanılarak yapılan modellemede etkin sonuçlar elde edilmiş, ancak yüksek donanım ihtiyacı gerekmesi de javantajlı bir durum oluşturmuştur.

Akıllı saldırı tespit sistemi oluşturmada kullanılan veri setlerinden KDD’99 veri seti diğer veri setlerine göre daha detaylıdır. Ancak veri tekrarının çok olması ve veri setinin büyük olması beraberinde verinin işlenmesi gibi sorunlar meydana getirmektedir.

Oluşturacak modelde girdilerin iyi seçilmesi modelinin karmaşıklığını ve sistem kaynağı ihtiyacını doğrudan etkilemektedir. Bu nedenle mümkün olduğu kadar az parametre ile doğru sonuca ulaşmak gerekmektedir. Bunun için parametre-özellik seçimi önem arz etmektedir.

YSA algoritmasında modelin eğitilmesi için gerekli olan eğitim ve doğrulama veri setindeki örneklem sayısının az olması modelin başarısını olumsuz yönden etkilemektedir. U2R ve R2L saldırılarına ait eğitim ve test verisinin az olması modelin başarısını olumsuz yönde etkilemiştir. Buna karşın örneklem sayısı en yüksek oranda olan DoS türündeki saldırıların %100’e yakın olacak şekilde doğru tahmin edilmesi bunu destekler mahiyettedir.

YSA’da gizli katman sayısı modelin başarısı üzerinde etkisi bulunmaktadır. KDD’99 veri seti özelinde bakıldığında belli bir gizli katman sayısından sonra modelin öğrenmeden çok ağın ezberlemesine neden olduğu görülmüştür.

YSA öğrenme algoritması sistem kaynağı ihtiyacını etkilemektedir. Levenberg-Marquard algoritması ile Bayesian Regularization algoritması karşılaştırıldığında Bayesian Regularization algoritması ile öğrenilen model daha başarılı sonuçlar ortaya koymuştur.

YSA'da KDD'99 veri setinde bulunan tüm özelliklerin kullanılması sonucunda en başarılı sonuçlar elde edilmiştir. Tüm özelliklerin kullanılması sistem kaynağı ihtiyacını artırmaktadır.

Eleme yapılan bazı özelliklerin modelden çıkarılması modelin karmaşıklığını düşürmekle birlikte U2R ve R2L saldırı türlerinin tespitinde noktasında olumsuz sonuçlar vermesine neden olmaktadır.

Literatürdeki çalışmalardan farklı olarak bağlantının saldırı olup-olmadığının tespitinin yapılması çalışmaya özgünlük kazandırmıştır.

YSA ve DT, ağa yapılan saldırıları tespit etmede etkili modelleme araçlarındandır.

Tezde uygulanan metodolojinin etkin sonuçları itibari ile katma değeri yüksek ürünlerin üretimine katkı sunması beklenmektedir.

6.2 Öneriler

Sonraki araştırmacılar aşağıda belirtilen konularda araştırmalar yapması uygun olacaktır.

- Türkiye'deki USOM ile siber güvenlik konusunda iyi durumda olan diğer ülkelerin USOM benzeri yapıların karşılaştırılması,
- Ülke çapında kritik önemde bulunan kurumsal yapılarda siber güvenlik stratejilerinin karşılaştırılması,
- Ülkemizdeki kritik yapılardaki kurumların siber güvenlik adına alınan önlemler ile siber güvenlik konusunda iyi durumda olan diğer ülkelerin kritik yapıların almış oldukları önlemlerin karşılaştırılması
- Akıllı saldırı tespit sistemlerinin birbirlerine göre avantaj ve dezavantajlarının karşılaştırılması,
- Verinin sınıflandırma işleminin tezimde uyguladığım öğrenme algoritmaları dışında farklı modellerin kullanılması,

- Tespit edilen saldırılara karşı otomatik işlem yapılması konularında araştırma yapılabilir.
- KDD veri setinin farklı sınıflandırma algoritmaları ile test edilmesi ve uygun olan modelin tespitinin yapılması.
- KDD'99 veri setindeki bazı saldırıların artık güncelliğini yitirdiği ve bazı saldırıların da ilgili veri setinde bulunmaması nedeni ile saldırı tespit ve saldırı önleyici sistemlerinde kullanmak üzere güncel veri setinin oluşturmak.
- KDD'99 veri setinin sadece TCP bağlantı özelliklerinden oluşan parametrelerin kullanılarak modelin eğitimindeki başarının ortaya konulması.
- Oluşturulacak modele tezimde elimine ettiğim değişkenler dışında başka değişkenlerin elimine edilip doğruluk oranlarının karşılaştırılması.
- Ağın eğitilmesi sonrası test işleminin bağımsız yapılabilmesi için KDD'99 veri seti dışından farklı bir test veri setinin oluşturulması.

6. KAYNAKÇA

- Halil BAYRAK, 2019, *2019 Dünya İnternet, Sosyal Medya ve Mobil Kullanıcı İstatistikleri*. <https://dijilopedi.com/2019-internet-kullanimi-ve-sosyal-medya-istatistikleri/> [Ziyaret Tarihi: 4 Kasım 2020]
- Anonim, 2016, *2016-2019 Ulusal Siber Güvenlik Stratejisi*, <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf> [Ziyaret Tarihi: 4 Kasım 2020].
- Anonim, 2018, *Sonicwall Siber Tehdit Raporu*, http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf [Ziyaret Tarihi: 4 Kasım 2020].
- Anonymous, 2020, *USMA CDX Network*, https://www.westpoint.edu/sites/default/files/inline-images/centers_research/cyber_research_center/PDFs/CDX_2009_Network_USMA.pdf [Ziyaret Tarihi: 4 Eylül 2020]
- Anonymous, 2020, *What Is Cybersecurity*, <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html> [Ziyaret Tarihi: 4 Eylül 2020].
- Djamel Khadraoui, Francine Herrmann, 2007, *Advances In Enterprise Information Technology Security*, Published in the United States of America by Information Science Reference, vol.1, pp. 1–19.
- Preeti Aggarwal and Sudhir Kumar Sharma, 2015, *Analysis of KDD Dataset Attributes- Class wise For Intrusion Detection*.
- K. Jayshree and R. S., 2012 “*Intrusion detection using data mining approach*,” *International Journal of Science and Research (IJSR)*, vol. 3, no. 11, pp.
- M. Erol, 2005, *Saldırı Tespit Sistemlerinde İstatistiksel Anormallik Belirleme Kullanımı*, ITÜ,
- Haluk Tanrikulu, Dr. Murat H. Sazlı, 2009, *Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması*, <https://dspace.ankara.edu.tr/xmlui/bitstream/handle/20.500.12575/30423/Haluk%2520TANRIKULU.pdf?sequence=1&isAllowed=y>, [Ziyaret Tarihi: 4 Eylül 2020].
- A. Hussain, J. Heidemann, C. Papadopoulos, 2004, “*Distinguishing between Singnal and Multisource Attacks Using Signal Processing*”, *Computer Networks*, vol. 46.
- Heba F. Eid¹, Ashraf Darwish², Aboul Ella Hassanien³, and Ajith Abraham, 2010, *Principle Components Analysis and Support Vector Machinebased Intrusion Detection System*.
- Pratibha Soni, Prabhakar Sharma, 2014, *An Intrusion Detection System Based on KDD-99 Data using Data Mining Techniques and Feature Selection*, *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume-4 Issue-3, July 2014

- Jiankun Hu, 2014, "A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns", IEEE Transactions on Computers, vol.63, no. 4, pp. 807-819.
- Aditya Harbola, Jyoti Harbola, Kunwar Singh Vaisla, 2014, *Improved Intrusion Detection in DDoS Applying feature selection Using Rank & Score of Attributes in KDD-99 data set.*
- P. Gifty Jeya, M. Ravichandran, C. S. Ravichandran, 2012, *Efficient Classifier for R2L and U2R Attacks.*
- Ibrahim M. Obeida, Nabhan Hamadneh, Mouhammd Alkasassbeh, Mohammad Almseidin, Mazen Ibrahim AlZubi, 2019, *Intensive Pre-Processing of KDD Cup 99 for Network Intrusion Classification Using Machine Learning Techniques.*
- Guy Bruneau, 2020, *The History and Evolution of Intrusion Detection,*
- Aarshay Jain, 2016, *Fundamentals of Deep Learning – Starting with Artificial Neural Network.*
- A. SARAVANAN and S. SATHYA BAMA, 2019, *A Review on Cyber Security and the Fifth Generation Cyberattacks, Oriental Journal of Computer Science and Technology, ISSN: 0974-6471, Vol. 12, No. (2) 2019, Pg. 50-56.*
- Nehinbe, J. O. 2011, *A critical evaluation of datasets for investigating idss and ipss researches,* In IEEE 10th International Conference on CIS, Page 92–97
- McHugh, J. 2000, *Testing intrusion detection systems: A critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory,* ACM Trans. Inf. Syst. Secur., 3(4):262–294.
- Iman Sharafaldin, Arash Habibi Lashkari and Ali A. Ghorbani, 2018, *Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization.*
- Nehinbe, J. O. 2010, *A Simple Method for Improving Intrusion Detections in Corporate Networks,* pages 111–122. Springer Berlin Heidelberg.
- Anonymous, 2002, *The CAIDA OC48 Peering Point Traces,* https://www.caida.org/data/passive/passive_oc48_dataset.xml [Ziyaret Tarihi: 4 Ağustos 2020]
- Nechaev, B., Allman, M., Paxson, V., and Gurtov, A., 2004, *Lawrence berkeley national laboratory(lbni)/icsi enterprise tracing Project.*
- Sangster, B., OConnor, T. J., Cook, T., Fanelli, R., Dean, E., Adams, W. J., Morrell, C., and Conti, G. . 2009, *Toward instrumenting network warfare competitions to generate labeled datasets. In 2009 Usenix. Usenix: The Advanced Computing System Association.*

- Sperotto, A., Sadre, R., Vliet, F., and Pras, A., 2009, *A labeled data set for flow-based intrusion detection*, In Proceedings of the 9th IEEE International Workshop on IP Operations and Management IPOM09, Sayfa 39–50.
- Swagatika Prusty, B. N. L. and Liberatore, M., 2011, *Forensic Investigation of the OneSwarm Anonymous Filesharing System*. In *ACM Conference on CCS*.
- Ali Shiravi, Hadi Shiravi, M. T. and Ghorbani, A. A. 2012. *Toward developing a systematic approach to generate benchmark datasets for intrusion detection*. *Computers and Security*, 31(3):357 – 374.
- M., Hu, J., and Slay, J., 2014, *Evaluating host-based anomaly detection systems: Application of the oneclass svm algorithm to adfa-ld*, In 2014 11th FSKD, pages 978–982.
- Salvatore J. Stolfo, Wei Fan, Wenke Lee, Andreas Prodromidis, and Philip K. Chan, *Intrusion Detector Learning*, <http://kdd.ics.uci.edu/databases/kddcup99/task.html> [Ziyaret Tarihi: 15 Ağustos 2020].
- Aditya Harbola, Jyoti Harbola, Kunwar Singh Vaisla, 2014, *Improved Intrusion Detection in DDoS Applying feature selection Using Rank & Score of Attributes in KDD-99 data set*.
- Hebb, Donald, 1949, *The Organization of Behavior*. New York: Wiley. ISBN 978-1-135-63190-1.
- Schmidhuber, J., 2015, *"Deep Learning in Neural Networks: An Overview"*. *Neural Networks*. 61: 85–117.
- Ivakhnenko Aleksei Grigor'evich, Valentin Grigor'evich Lapa, 1965, *Cybernetic Predicting Devices*. CCM Information Corporation.
- Maad M. Mijwil, 2018, *Artificial Neural Networks Advantages and Disadvantages*. https://www.researchgate.net/profile/Maad_Mijwil/publication/323665827_Artificial_Neural_Networks_Advantages_and_Disadvantages/links/5aa2c01faca272d448b5a23d/Artificial-Neural-Networks-Advantages-and-Disadvantages.pdf [Ziyaret Tarihi: 15 Ekim 2020].
- Aslı Çalış, Sema Kayapınar, Tahsin Çetinyokuş, 2014, *Veri Madenciliğinde Karar Ağacı Algoritmaları ile Bilgisayar ve İnternet Güvenliği Üzerine Bir Uygulama*. *Endüstri Mühendisliği Dergisi* Cilt: 25 Sayı: 3-4 Sayfa: (2-119)
- Anonim, 2020, *Decision Trees*, Decision tree - Wikipedia, https://en.wikipedia.org/wiki/Decision_tree_learning [Ziyaret Tarihi: 15 Ağustos 2020].
- Akdemir, B., Güneş, S. and Genç, A., 2009, *Artificial neural network training models in prediction of concrete compressive strength using euclidean normalization method*, 3rd *Int. Conf. on Complex Systems and Applications-ICCSA 2009*, Le Havre-France, 160-165.

- Adel Jahanbani and Hossein Karimi, 2012, “A new approach for detecting intrusions based on the PCA neural networks”, Journal of Basic and Applied Scientific Research, pp. 672-679, 2012.
- R. Agarwal and M. V. Joshi, 2000, “PNrule: A new framework for learning classifier models in data mining (A case study in Network Intrusion Detection), IBM research division technical report no. RC-21719.
- H. Gunes Kayacik, A. Nur Zincir Heywood and I. Heywood, 2007, “An hierarchical SOM-based intrusion detection” in Journal on Engineering Applications of Artificial Intelligence, Vol. 20, pp. 439-451.
- P. Gifty Jeya, M. Ravichandran, C. S. Ravichandran, 2012, Efficient Classifier for R2L and U2R Attacks, International Journal of Computer Applications (0975 – 8887) Volume 45–No.21, May.
- Kamiński, B.; Jakubczyk, M.; Szufel, P, 2017. A framework for sensitivity analysis of decision trees. Central European Journal of Operations Research. 26 (1): 135–15
- VAN DIEPEN, Merel ve Philip Hans FRANCES, 2006, *Evaluating Chi-Squared Automatic Interaction Detection*, Information Systems, 31, No. 8, 2006.
- Deng, H.; Runger, G.; Tuv, E. 2011. Bias of importance measures for multi-valued attributes and solutions. Proceedings of the 21st International Conference on Artificial Neural Networks (ICANN).
- Anonim, 2020, *Firewall nedir? Nasıl Çalışır? KOBİ’ler Hangi Tür Firewall’u Kullanmalıdır.*, <https://berqnet.com/blog/firewall-nedir>, [Ziyaret Tarihi: 19 Ağustos 2020]
- Anonim, 2020, *rootkit nedir rootkit programlama ve rootkit virüsü*, <https://wmaraci.com/nedir/rootkit>, [Ziyaret Tarihi: 19 Ağustos 2020]
- Alex Perekalin, 2017, *Wannacry: Güvende misiniz*, <https://www.kaspersky.com.tr/blog/wannacry-ransomware/3181/>, [Ziyaret Tarihi: 19 Ağustos 2020]
- Mike Mcquade, 2018, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>, [Ziyaret Tarihi: 19 Ağustos 2020].
- Anonim, 2017, *Stuxnet*, Decision tree - Wikipedia, <https://tr.wikipedia.org/wiki/Stuxnet> [Ziyaret Tarihi: 15 Ağustos 2020].
- Anonim, 2020, *Darkhotel kötü amaçlı yazılım virüs tehdidi*, <https://www.kaspersky.com.tr/resource-center/threats/darkhotel-malware-virus-threat-definition> [Ziyaret Tarihi: 15 Ağustos 2020].
- Nicky Woolf, 2016, *Major cyber attack disrupts internet service across Europe and US*, <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>, [Ziyaret Tarihi: 19 Ağustos 2020].

Anonim, 2013, *USOM Hakkında*, <https://www.usom.gov.tr/hakkimizda.html> [Ziyaret Tarihi: 15 Temmuz 2020].

Anonim, 2017, *USOM ve Ulusal Olaylara Müdahale Ekibi*, <https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi> [Ziyaret Tarihi: 15 Temmuz 2020].

Anonim, 2014, *Kurumsal SOME Kurulum ve Yönetim Rehberi*, https://www.usom.gov.tr/dosya/1470336377-Kurumsal%20_SOME_Rehberi.pdf [Ziyaret Tarihi: 19 Temmuz 2020].

İTU BİDB, 2013, *OSI Katmanları*, <https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/osi-katmanlar%c4%b1> [Ziyaret Tarihi: 19 Temmuz 2020].

Anonim, 2012, *OSI Modeli*, https://tr.wikipedia.org/wiki/OSI_modeli#4._Katman:_Ta%C5%9F%C4%B1ma/iletim_Katmanı [Ziyaret Tarihi: 19 Temmuz 2020].

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Hanifi TOPRAK
Uyruğu : T.C.
Doğum Yeri ve Tarihi :
Telefon :
Faks :
e-mail :

EĞİTİM

Derece	Adı, İlçe, İl	Bitirme Yılı
Lise	: Batman Anadolu Lisesi, Merkez, Batman	2004
Üniversite	: Mersin Üniversitesi, Merkez, Mersin	2008
Yüksek Lisans	: Batman Üniversitesi, Merkez, Batman	2021
Doktora	:	

İŞ DENEYİMLERİ

Yıl	Kurum	Görevi
2008-2009	Milli Eğitim Müdürlüğü	Bilgisayar Öğretmeni
2009-2012	Harran Üniversitesi	Mühendis
2012-	Batman Üniversitesi	Mühendis
2019-	Batman Üniversitesi	Şube Müdür V.

UZMANLIK ALANI

Sistem Yöneticiliği
 Network Yöneticiliği
 Siber Güvenlik
 Big Data
 Yapay Zeka
 Web Programlama
 IP Camera

YABANCI DİLLER

İngilizce
 Almanca

YAYINLAR

Hanifi TOPRAK, Suleyman Kardaş, 2020, 2. Katman İç Ağ Saldırıları Ve Önlemler, ISPEC 6th INTERNATIONAL CONFERENCE ON ENGINEERING & NATURAL SCIENCES, ISBN: 978-605-7811-49-3, Pages: 222-238

Hanifi TOPRAK, Suleyman Kardaş, 2020, *KDD Veri Setindeki Siber Saldırıları*, ISPEC 6th INTERNATIONAL CONFERENCE ON ENGINEERING & NATURAL SCIENCES, ISBN: 978-605-7811-48-6, Page: 117