T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SİBER FİZİKSEL VE ENDÜSTRİYEL SİSTEMLERDE DAVETSİZ MİSAFİR SALDIRILARININ ANORMALLİK TESPİTİ İÇİN YAPAY ZEKA VE YUMUŞAK HESAPLAMA YÖNTEMLERİNİN UYGULANMASI

SİNAN ATICI

YÜKSEK LİSANS TEZİ

MEKATRONİK MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Prof. Dr. Gürkan TUNA

EDİRNE-2025

Sinan Atıcı'nın hazırladığı **"SİBER FİZİKSEL VE ENDÜSTRİYEL SİSTEMLERDE DAVETSİZ MİSAFİR SALDIRILARININ ANORMALLİK TESPİTİ İÇİN YAPAY ZEKA VE YUMUŞAK HESAPLAMA YÖNTEMLERİNİN UYGULANMASI"** başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından **Mekatronik Mühendisliği** Anabilim Dalında bir **Yüksek lisans tezi** olarak kabul edilmiştir.

Jüri Üyeleri	İmza
Prof. Dr. Gürkan TUNA	……
Doç. Dr. Hayrettin TOYLAN	……
Dr. Öğr. Üyesi M. Ozan AKI	……

Tez Savunma Tarihi: 03/07/2025

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Prof. Dr. Gürkan TUNA

Tez Danışmanı ……

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

……

Doç. Dr. Filiz UMAROĞULLARI

Fen Bilimleri Enstitüsü Müdürü

TRAKYA ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ

MEKATRONİK MÜHENDİSLİĞİ ANABİLİM DALI YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

03 / 07/ 2025

Sinan ATICI

İmza

Yüksek Lisans Tezi

SİBER FİZİKSEL VE ENDÜSTRİYEL SİSTEMLERDE DAVETSİZ MİSAFİR SALDIRILARININ ANORMALLİK TESPİTİ İÇİN YAPAY ZEKA VE YUMUŞAK HESAPLAMA YÖNTEMLERİNİN UYGULANMASI

Trakya Üniversitesi, Fen Bilimleri Enstitüsü

Mekatronik Mühendisliği Anabilim Dalı

ÖZET

Siber-fiziksel sistemler ve endüstriyel kontrol sistemlerinin dijitalleşmesi, bu sistemlere yönelik siber tehditlerin karmaşıklığını ve tehlikelerini artırmıştır. Özellikle davetsiz misafir saldırıları, sistemlerin sürekliliği ve güvenliği üzerinde ciddi bir tehdit oluşturmaktadır. Bu tez çalışmasında, siber-fiziksel sistemler ve endüstriyel kontrol sistemlerinde davetsiz misafir saldırılarının anomali tespiti için yapay zeka ve yumuşak hesaplama temelli yöntemlerin performansı sistematik bir şekilde incelenmiştir. Bu amaçla, CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset gibi güncel ve kapsamlı veri setleri kullanılarak çeşitli makine öğrenmesi, derin öğrenme ve yumuşak hesaplama teknikleri uygulanmıştır. Karar ağaçları, destek vektör makineleri, K-en yakın komşu, lojistik regresyon ve doğrusal diskriminant analizi gibi klasik makine öğrenmesi algoritmaları ile Evrişimli Sinirsel Ağ ve Uzun Kısa Dönemli Bellek gibi derin öğrenme yaklaşımlarının performansı değerlendirilmiştir. Ayrıca, bulanık mantık, Genetik Algoritmalar, Uyarlamalı Nöro-Bulanık Çıkarım Sistemi ve Derin Q Ağı gibi yumuşak hesaplama yöntemleriyle hem bağımsız hem de hibrit modeller geliştirilerek sistem performansı analiz edilmiştir. Elde edilen bulgular, klasik makine öğrenmesi modellerinin genellikle yüksek isabetlilik sunduğunu, ancak derin öğrenme ve yumuşak hesaplama temelli yöntemlerin, özellikle azınlık sınıflarında ve karmaşık veri setlerinde esneklik ve uyarlanabilirlik avantajları sağladığını ortaya koymaktadır. Çalışma, bu yöntemlerin siber-fiziksel ve endüstriyel kontrol sistemlerindeki uygulanabilirliğini

göstermeyi ve bu alanda yapılacak ileri düzey araştırmalara katkı sunmayı hedeflemektedir.

Yıl : 2025

Sayfa Sayısı: 195

Anahtar Kelimeler: Siber Fiziksel Sistemler, Anomali Tespiti, Yumuşak Hesaplama, Yapay Zeka, Siber Güvenlik

Master's Thesis

APPLICATION OF ARTIFICIAL INTELLIGENCE AND SOFT COMPUTING METHODS FOR ANOMALY DETECTION OF INTRUSION ATTACKS IN CYBER-PHYSICAL AND INDUSTRIAL SYSTEMS

Trakya University, Institute of Natural and Applied Sciences

Department of Mechatronics Engineering

ABSTRACT

The digitisation of cyber-physical systems and industrial control systems has amplified the complexity and severity of cyber threats targeting these systems. In particular, intrusion attacks pose a significant threat to the continuity and security of such systems. This thesis investigates the performance of artificial intelligence and soft computing-based methods for anomaly detection of intrusion attacks in cyber-physical and industrial control systems through a systematic approach. To this end, contemporary and comprehensive datasets, namely CIC-ToN-IoT, CSE-CIC-IDS2018, and Edge-IIoTset, were employed to apply various machine learning, deep learning, and soft computing techniques. The performance of classical machine learning algorithms, including decision trees, support vector machines, K-nearest neighbour, logistic regression, and linear discriminant analysis, was evaluated alongside deep learning approaches such as Convolutional Neural Networks and Long Short-Term Memory networks. Furthermore, soft computing methods, including fuzzy logic, Genetic Algorithms, Adaptive Neuro-Fuzzy Inference Systems, and Deep Q Networks, were used to develop both standalone and hybrid models, with their system performance thoroughly analysed. The findings reveal that classical machine learning models generally achieve high accuracy, while deep learning and soft computing-based methods offer advantages in flexibility and adaptability, particularly for minority classes and complex datasets. This

study aims to demonstrate the applicability of these methods in cyber-physical and industrial control systems and to provide a foundation for advanced research in this field.

Year 2025

Number of Pages: 195

Keywords: Cyber-Physical Systems, Anomaly Detection, Soft Computing, Artificial Intelligence, Cybersecurity

İÇİNDEKİLER

ÖZET iv
ABSTRACT vi
İÇİNDEKİLER viii
ŞEKİLLER DİZİNİ xi
ÇİZELGELER DİZİNİ xvii
BÖLÜM 1 1
1. GİRİŞ 1
BÖLÜM 2 4
2. LİTERATÜR İNCELEMESİ 4
2.1. Siber Fiziksel ve Endüstriyel Sistemler 4
2.2. İlgili Çalışmalar 9
2.3. Hesaplama Paradigmaları 12
2.3.1. Bulanık Mantık ve Uyarlamalı Nöro-Bulanık Çıkarım Sistemi (ANFIS) 15
2.3.2. Genetik Algoritmalar (GA) 16
2.3.3. Pekiştirmeli Öğrenme (RL) ve Derin Q Ağı (DQN) 16
2.3.4. Karar Ağaçları 18
2.3.5. Doğrusal Diskriminant Analizi (LDA) 19
2.3.6. Lojistik Regresyon 19
2.3.7. Naive Bayes 19

2.3.8. Destek Vektör Makineleri (SVM) 20
2.3.9. K-En Yakın Komşu (KNN) 20
2.3.10. Evrişimli Sinirsel Ağ (CNN) Algoritması 20
2.3.11. Uzun Kısa Dönemli Bellek (LSTM) Algoritması 21
2.4. Gerçek Veri Setlerinin Toplanması ve Seçilmesi 21
BÖLÜM 3 24
3. MATERYAL ve YÖNTEM 24
3.1. Yöntemlerin Matematiksel Modelleri 24
3.1.1. Bulanık Mantık 24
3.1.2. Uyarlamalı Nöro-Bulanık Çıkarım Sistemi (ANFIS) 26
3.1.3. Genetik Algoritmalar 28
3.1.4. Pekiştirmeli Öğrenme ve Derin Q Ağı (DQN) 30
3.1.5. Karar Ağaçları 37
3.1.6. Doğrusal Diskriminant Analizi (LDA) 40
3.1.7. Lojistik Regresyon 43
3.1.8. K-En Yakın Komşu (KNN) 46
3.2. Veri Setlerinin İncelenmesi ve Hazırlanması 49
3.2.1. CIC-ToN-IoT Veri Seti 50
3.2.2. CSE-CIC-IDS2018 Veri Seti 54
3.2.3. Edge-IIoTset Veri Seti 58
BÖLÜM 4 63
4. SONUÇLAR 63
4.1. CIC-ToN-IoT Veri Seti ile Elde Edilen Bulgular 63
4.2. CSE-CIC-IDS2018 Veri Seti ile Elde Edilen Bulgular 94
4.3. Edge-IIoTset Veri Seti ile Elde Edilen Bulgular 125

4.4. Elde Edilen Bulguların Karşılaştırılması 156
BÖLÜM 5 160
TARTIŞMA 160
KAYNAKLAR 164
TEZ ÖĞRENCİSİNE AİT BİLİMSEL ÇIKTILAR 175
ÖZGEÇMİŞ 176

ŞEKİLLER DİZİNİ

Şekil 2.1. Hesaplama paradigmalarının sınıflandırılması (Falcone vd., 2020)..... 13

Şekil 2.2. ANFIS modeli yapısı 16

Şekil 2.3. Pekiştirmeli öğrenme çevrimi..... 17

Şekil 3.1. CIC-ToN-IoT veri setinde özellikler arası korelasyon matrisi 50

Şekil 3.2. CIC-ToN-IoT veri setinde çoklu etiketli sınıf dağılımı..... 51

Şekil 3.3. CIC-ToN-IoT veri setinde çoklu etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri) 52

Şekil 3.4. CIC-ToN-IoT veri setinde ikili etiketli sınıf dağılımı 52

Şekil 3.5. CIC-ToN-IoT veri setinde ikili etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)..... 53

Şekil 3.6. CSE-CIC-IDS2018 veri setinde özellikler arası korelasyon matrisi 54

Şekil 3.7. CSE-CIC-IDS2018 veri setinde çoklu etiketli sınıf dağılımı. 55

Şekil 3.8. CSE-CIC-IDS2018 veri setinde çoklu etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri) 56

Şekil 3.9. CSE-CIC-IDS2018 veri setinde ikili etiketli sınıf dağılımı..... 56

Şekil 3.10. CSE-CIC-IDS2018 veri setinde ikili etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri) 57

Şekil 3.11. Edge-IIoT veri setinde özellikler arası korelasyon matrisi..... 58

Şekil 3.12. Edge-IIoT veri setinde çoklu etiketli sınıf dağılımı..... 59

Şekil 3.13. Edge-IIoT veri setinde çoklu etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)..... 60

Şekil 3.14. Edge-IIoT veri setinde ikili etiketli sınıf dağılımı 61

Şekil 3.15. CSE-CIC-IDS2018 veri setinde ikili etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri) 61

Şekil 4.1. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin ikili etiket t-SNE grafiği 69

Şekil 4.2. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin ikili etiket karmaşıklık matrisi 70

Şekil 4.3. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin çoklu etiket t-SNE grafiği 71

Şekil 4.4. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin çoklu etiket karmaşıklık matrisi 72

Şekil 4.5. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin ikili etiket t-SNE grafiği 74

Şekil 4.6. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin ikili etiket karmaşıklık matrisi 75

Şekil 4.7. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket t-SNE grafiği 76

Şekil 4.8. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket karmaşıklık matrisi 77

Şekil 4.9. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin ikili etiket t-SNE grafiği 79

Şekil 4.10. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin ikili etiket Karmaşıklık matrisi 80

Şekil 4.11. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin çoklu etiket t-SNE grafiği 81

Şekil 4.12. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin çoklu etiket karmaşıklık matrisi 82

Şekil 4.13. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket t-SNE grafiği 85

Şekil 4.14. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket karmaşıklık matrisi 86

Şekil 4.15. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket t-SNE grafiği 87

Şekil 4.16. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket karmaşıklık matrisi 88

Şekil 4.17. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket t-SNE grafiği 90

Şekil 4.18. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket karmaşıklık matrisi 91

Şekil 4.19. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket t-SNE grafiği 92

Şekil 4.20. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket karmaşıklık matrisi 93

Şekil 4.21. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin ikili etiket t-SNE grafiği 100

Şekil 4.22. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin ikili etiket karmaşıklık matrisi 101

Şekil 4.23. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin çoklu etiket t-SNE grafiği 102

Şekil 4.24. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin çoklu etiket karmaşıklık matrisi 103

Şekil 4.25. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin ikili etiket t-SNE grafiği 105

Şekil 4.26. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin ikili etiket karmaşıklık matrisi 106

Şekil 4.27. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket t-SNE grafiği 107

Şekil 4.28. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket karmaşıklık matrisi 108

Şekil 4.29. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin ikili etiket t-SNE grafiği 111

Şekil 4.30. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin ikili etiket karmaşıklık matrisi 112

Şekil 4.31. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin çoklu etiket t-SNE grafiği 113

Şekil 4.32. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin çoklu etiket karmaşıklık matrisi 114

Şekil 4.33. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket t-SNE grafiği 117

Şekil 4.34. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket karmaşıklık matrisi 118

Şekil 4.35. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket t-SNE grafiği 119

Şekil 4.36. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket karmaşıklık matrisi 120

Şekil 4.37. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket t-SNE grafiği 122

Şekil 4.38. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket karmaşıklık matrisi 123

Şekil 4.39. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket t-SNE grafiği 124

Şekil 4.40. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket karmaşıklık matrisi 125

Şekil 4.41. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin ikili etiket t-SNE grafiği 132

Şekil 4.42. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin ikili etiket karmaşıklık matrisi 133

Şekil 4.43. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin çoklu etiket t-SNE grafiği 134

Şekil 4.44. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin çoklu etiket karmaşıklık matrisi 135

Şekil 4.45. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin ikili etiket t-SNE grafiği 137

Şekil 4.46. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin ikili etiket karmaşıklık matrisi 138

Şekil 4.47. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket t-SNE grafiği 139

Şekil 4.48. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket karmaşıklık matrisi 140

Şekil 4.49. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin ikili etiket t-SNE grafiği 142

Şekil 4.50. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin ikili etiket karmaşıklık matrisi 143

Şekil 4.51. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin çoklu etiket t-SNE grafiği 144

Şekil 4.52. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin çoklu etiket karmaşıklık matrisi 145

Şekil 4.53. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket t-SNE grafiği 148

Şekil 4.54. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket karmaşıklık matrisi 149

Şekil 4.55. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket t-SNE grafiği 150

Şekil 4.56. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket karmaşıklık matrisi 151

Şekil 4.57. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket t-SNE grafiği 153

Şekil 4.58. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket karmaşıklık matrisi 154

Şekil 4.59. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket t-SNE grafiği 154

Şekil 4.60. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket karmaşıklık matrisi 155

ÇİZELGELER DİZİNİ

Çizelge 4.1. CIC-ToN-IoT Veri Setine Ait Öznitelik ve Sınıf Dağılımı 63

Çizelge 4.2. CIC-ToN-IoT Veri Seti Üzerinde Makine Öğrenmesi Modellerinin Performans Karşılaştırması 65

Çizelge 4.3. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan Derin Öğrenme Tabanlı Yöntemler 67

Çizelge 4.4. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan CNN Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 68

Çizelge 4.5. CIC-ToN-IoT Veri Seti Üzerinde kullanılan LSTM Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 72

Çizelge 4.6. CIC-ToN-IoT Veri Seti Üzerinde kullanılan Yumuşak Hesaplama Tabanlı Yöntemler 77

Çizelge 4.7. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan GA Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 78

Çizelge 4.8. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan Hibrit Tabanlı Yöntemler ... 82

Çizelge 4.9. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan ANFIS Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 83

Çizelge 4.10. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan Pekiştirmeli Öğrenme Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 88

Çizelge 4.11. CSE-CIC-IDS2018 Veri Setine Ait Öznitelik ve Sınıf Dağılımı 94

Çizelge 4.12. CSE-CIC-IDS2018 Veri Seti Üzerinde Makine Öğrenmesi Modellerinin Performans Karşılaştırması 95

Çizelge 4.13. CSE-CIC-IDS2018 Veri Seti Üzerinde kullanılan Derin Öğrenme Tabanlı Yöntemler 98

Çizelge 4.14. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan CNN Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 98

Çizelge 4.15. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan LSTM Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 104

Çizelge 4.16. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan Yumuşak Hesaplama Tabanlı Yöntemler 109

Çizelge 4.17. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan GA Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 109

Çizelge 4.18. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan Hibrit Tabanlı Yöntemler 115

Çizelge 4.19. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan ANFIS Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 115

Çizelge 4.20. CSE-CIC-IDS2018 Veri Seti Üzerinde kullanılan Pekiştirmeli Öğrenme Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 121

Çizelge 4.21. Edge-IIoTset Veri Setine Ait Öznitelik ve Sınıf Dağılımı 126

Çizelge 4.22. Edge-IIoTset Veri Seti Üzerinde Makine Öğrenmesi Modellerinin Performans Karşılaştırması 127

Çizelge 4.23. Edge-IIoTset Veri Seti Üzerinde Kullanılan Derin Öğrenme Tabanlı Yöntemler 130

Çizelge 4.24. Edge-IIoTset Veri Seti Üzerinde Kullanılan CNN Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 130

Çizelge 4.25. Edge-IIoTset Veri Seti Üzerinde Kullanılan LSTM Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 135

Çizelge 4.26. Edge-IIoTset Veri Seti Üzerinde Kullanılan Yumuşak Hesaplama Tabanlı Yöntemler 140

Çizelge 4.27. Edge-IIoTset Veri Seti Üzerinde Kullanılan GA Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 141

Çizelge 4.28. Edge-IIoTset Veri Seti Üzerinde Kullanılan Hibrit Tabanlı Yöntemler 145

Çizelge 4.29. Edge-IIoTset Veri Seti Üzerinde Kullanılan ANFIS Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri..... 146

Çizelge 4.30. Edge-IIoTset Veri Seti Üzerinde Kullanılan Pekiştirmeli Öğrenme Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri 151

Çizelge 4.31. Modellerin CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset Veri Setleri Üzerindeki Test İsabetlilik (%) Değerleri (İkili / Çoklu Etiket) 157

BÖLÜM 1

1. GİRİŞ

Endüstriyel kontrol sistemleri (ICS), enerji şebekeleri ve fabrika otomasyonu gibi endüstriyel süreçleri izlemek ve kontrol etmek için tasarlanmış, genellikle Veri Tabanlı Kontrol ve Gözetleme Sistemi (SCADA), Dağıtık Kontrol Sistemi (DCS) ve Programlanabilir Mantıksal Denetleyici (PLC) gibi donanımları içeren ve geleneksel olarak fiziksel izolasyonla güvenliği sağlanan sistemlerdir (Kayan vd., 2022). Siber-Fiziksel Sistemler (CPS), hesaplama ve fiziksel bileşenleri entegre ederek ulaşım, sağlık ve akıllı şehirler gibi alanlarda gerçek zamanlı izleme ve kontrol sağlayan, Nesnelerin İnterneti (IoT) gibi teknolojilerle desteklenen daha geniş bir sistem kategorisidir (Oks vd., 2024; El-Kady vd., 2023). Endüstriyel CPS (ICPS), CPS'nin endüstriyel bağlamda uygulanmasıdır; dijitalleşme sayesinde verimlilik, otomasyon ve bağlantı artarken (dijital ikizler, bulut bilişim vb.), özellikle davetsiz misafir saldırılarına karşı ortaya çıkan yeni güvenlik açıkları bu sistemleri siber tehditlere daha savunmasız hale getirmiştir (Oks vd., 2024; Alcaraz & Lopez, 2022).

Anomaliler, bir sistemin normal işleyişinden sapma gösteren ve performans veya güvenlik açısından risk oluşturan beklenmedik değişiklikler olarak tanımlanabilir. IoT bağlamında, bu sapmalar, küresel veya yerel normların dışında gerçekleşen ve sistemin tipik çalışma özelliklerinden farklılık gösteren gözlemlenebilir etkiler şeklinde ortaya çıkar. Anomali tespiti, ağ operatörleri için kritik bir süreçtir ve özellikle trafik verilerindeki olağandışı eğilimlerin hızlı ve verimli bir şekilde belirlenmesini gerektirir. IoT sistemlerinde toplanan verilerin çoğu normal kabul edilse de, sistemin dinamik yapısı nedeniyle "normal" tanımı zamanla değişebilir. Geniş alanlara yayılmış düşük maliyetli

sensörlerden oluşan IoT ağları, merkezi, merkezi olmayan veya blokzincir tabanlı dağıtık yapılarda organize olabilir. Bu ağlardaki anomaliler, sensör arızalarından siber saldırılara (örneğin Hizmet Reddi (DoS), Dağıtık Hizmet Reddi (DDoS), veri sızıntısı ve dolandırıcılık) kadar geniş bir yelpazede tehditlere işaret edebilir (Abshari & Sridhar, 2025). Bu tür risklerin önlenmesi, yapay zeka (AI), makine öğrenimi ve derin öğrenme gibi gelişmiş tespit yöntemlerinin kullanımını zorunlu kılmaktadır (Khilar vd., 2022; Guato Burgos vd., 2024). Dolayısıyla, anomali tespiti, IoT sistemlerinin güvenilirliğini ve verimliliğini sağlamak amacıyla çeşitli alanlarda yaygın olarak uygulanmaktadır.

Yapay zeka tekniklerinin yanı sıra, yumuşak hesaplama yöntemleri de siber-fiziksel sistemlerde anomali tespit yeteneklerini güçlendirmede önemli bir rol oynamaktadır. Yumuşak hesaplama teknikleri, bulanık mantık, sinir ağları ve evrimsel algoritmalar dahil, anomali tespit sistemlerinin sağlamlığını ve adaptasyon yeteneğini artırmak için geleneksel makine öğrenimi yöntemleriyle giderek daha fazla entegre edilmektedir. (Datta Gupta vd., 2023; Thomas vd., 2023)

İzinsiz Giriş Tespit Sistemleri (IDS), ağ trafiğini analiz ederek anormallikleri tespit etmede kritik rol oynar. Ancak, imza tabanlı yaklaşımları nedeniyle sıfırıncı gün saldırılarını önlemede yetersiz kalır ve gerçek zamanlı çözüm sunmakta zorlanır. Fizik temelli sinir ağları (PbNN) gibi hibrit yaklaşımlar, fiziksel süreçlerin dinamiklerini derin öğrenme modelleriyle birleştirerek daha güvenilir anomali tespiti sağlamaktadır. Anomali tespiti, öğrenme ve anormal davranışları tanıma yeteneğiyle bu sorunlara potansiyel bir çözüm sunar. Fakat mevcut yaklaşımlar, genellikle gerçekçi olmayan veri kümeleriyle test edildiğinden pratikte yeterince etkili değildir (Al-Fuhaidi vd., 2024; Raman & Mathur, 2022; Martins vd., 2022).

Bu tez çalışmasında, CPS ve ICS davetsiz misafir saldırılarının anormallik tespiti için yapay zeka ve yumuşak hesaplama yöntemleri sistematik bir şekilde incelenmiştir. 2. Bölümde, literatür taraması yapılarak siber-fiziksel ve endüstriyel sistemler, ilgili çalışmalar ve makine zekâsı ile hesaplama paradigmaları arasında Bulanık Mantık, Uyarlamalı Nöro-Bulanık Çıkarım Sistemi (ANFIS), Genetik Algoritma (GA), Pekiştirmeli Öğrenme (RL), Derin Q Ağı (DQN), Karar Ağaçları, Doğrusal Diskriminant Analizi (LDA), Lojistik Regresyon, Destek Vektör Makineleri (SVM), K-en yakın komşu (KNN), Evrişimli Sinirsel Ağ (CNN), Uzun Kısa Dönemli Bellek (LSTM) detaylı bir

şekilde ele alınmış; ayrıca gerçek veri setlerinin toplanması incelenmiştir. 3. Bölümde, yöntemlerin matematiksel modelleri (Bulanık Mantık, ANFIS, GA, DQN, Karar Ağaçları, LDA, lojistik regresyon, KNN) geliştirilmiş, veri setleri (CIC-ToN-IoT, CSE-CIC-IDS2018, Edge-IIoTset) hazırlanmıştır. 4. Bölümde, elde edilen bulgular analiz edilerek CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset veri setleri üzerindeki performanslar değerlendirilmiştir. Çalışma, yöntemlerin hem kuramsal hem de pratik uygulanabilirliklerini değerlendirmeyi amaçlamıştır.

Elde edilen bulgular, farklı yöntemlerin anomali tespitinde benzersiz avantajlar sunduğunu ortaya koymuştur. Klasik makine öğrenimi algoritmaları, özellikle basit ve hızlı modellerle iyi sonuçlar vermiş, ancak karmaşık saldırılarda sınırlı kalmıştır. Derin öğrenme yaklaşımları (CNN ve LSTM), özellikle çoklu etiket sınıflandırmada yüksek doğruluk oranları sunarken, yumuşak hesaplama yöntemleri (ANFIS, GA) esneklik ve adaptasyon açısından öne çıkmıştır. Hibrit modeller, hem doğruluk hem de genelleme performansında umut verici sonuçlar vermiş; bu da gelecekte daha karmaşık sistemlere yönelik özelleştirilmiş hibrit yaklaşımların geliştirilmesinin gerekliliğini vurgulamaktadır. Sonuçlar, bu yöntemlerin siber-fiziksel sistemlerin güvenliğini artırmada potansiyel taşıdığını ve ileri araştırmalar için sağlam bir temel oluşturduğunu göstermiştir.

BÖLÜM 2

2. LİTERATÜR İNCELEMESİ

2.1. Siber Fiziksel ve Endüstriyel Sistemler

Bu bölümde, siber fiziksel ve endüstriyel sistemlerde karşılaşılan davetsiz misafir saldırılarına karşı geliştirilen mevcut koruma yaklaşımları, ilgili güvenlik protokolleri ve yapay zekâ temelli yöntemler kapsamlı bir şekilde incelenmiştir. Öncelikle siber güvenlik teorileri ve saldırı türleri ele alınmış, ardından bu tehditlerin özellikle endüstriyel sistemler üzerindeki etkilerine odaklanılmıştır. Literatürde yer alan çalışmalar doğrultusunda, yapay zekâ ve yumuşak hesaplama paradigmalarının bu tür sistemlerde anormallik tespiti amacıyla nasıl kullanıldığı değerlendirilmiştir. Ayrıca, kullanılan veri setlerinin niteliği ve seçim gerekçeleri açıklanmıştır. Bu bağlamda sunulan literatür incelemesi, çalışmanın metodolojik temelini oluşturarak ileri bölümlerde sunulacak modellemelere teorik bir zemin hazırlamaktadır.

Siber fiziksel ve endüstriyel sistemler, fiziksel süreçlerin dijital teknolojilerle entegre edilerek izlenmesi, kontrolü ve optimizasyonunu sağlayan kritik altyapılardır. Bu bölümde, Endüstriyel Nesnelerin İnterneti (IIoT), ICS, CPS ve ICPS kavramları ele alınacaktır.

CPS, fiziksel süreçlerle hesaplamalı bileşenlerin bütünleştiği, gömülü sistemler ve sensörler aracılığıyla fiziksel çevrenin izlenip kontrol edildiği, etkileşimli ve gerçek zamanlı yapılar sunar. Geleneksel ICS'den farklı olarak, CPS yalnızca endüstriyel süreçlerle sınırlı kalmayıp akıllı şebekeler, otonom araçlar ve akıllı binalar gibi daha geniş bir uygulama yelpazesini kapsar. Bu genişletilmiş kapsam, CPS'yi daha karmaşık hale getirirken aynı zamanda siber güvenlik açısından yeni zorluklar da doğurur. ICS'ler,

güvenlik, süreklilik ve güvenilirlik gibi endüstriyel öncelikler doğrultusunda şekillenmiş CPS alt kümeleri olarak değerlendirilebilir. Her iki yapı da fiziksel ve dijital bileşenlerin entegrasyonunu amaçlasa da, CPS daha yüksek düzeyde etkileşim, veri analitiği ve kontrol algoritmaları gerektirir. Bu nedenle CPS, hem kapsam hem de işlevsellik bakımından ICS'den daha gelişmiş bir sistem mimarisi sunar (Abshari & Sridhar, 2025).

IIoT, üretim süreçlerinde yer alan sensör, eyleyici ve cihazların internet üzerinden bağlantı kurarak veri alışverişi yapmasını sağlayan ve Endüstri 4.0'ın temel bileşenlerinden biri olan çok katmanlı bir altyapıdır. Bu yapı; fiziksel dünyadan veri toplayan IIoT sensör ve cihazlarının, verileri işleyip ileten ağ geçitleri aracılığıyla bulut ortamına aktarılması ve burada analiz edilerek akıllı üretim uygulamalarına (örneğin akıllı robotik, üretim optimizasyonu, duruş süresi azaltımı ve gelişmiş izleme) hizmet etmesi şeklinde işler. Ancak, bu katmanlı yapıda çok sayıda bağlı cihazın bulunması güvenlik risklerini artırmakta; bu nedenle güvenli ve esnek IIoT çözümlerinin geliştirilmesi kritik önem taşımaktadır (Wadsworth vd., 2019).

CPS, fiziksel süreçlerle dijital kontrol mekanizmalarının bütünleşik çalıştığı, veri toplama, işleme ve karar alma işlevlerini gerçek zamanlı olarak gerçekleştirebilen sistemlerdir. Bu yapı, gömülü yazılımlar ve ağlar aracılığıyla fiziksel dünyadan gelen verilerle etkileşime girerek çevresine uyum sağlayabilen, yeniden yapılandırılabilir ve öğrenme yeteneğine sahip sistemlerin temelini oluşturur. Endüstri 4.0 kapsamında CPS, yalnızca otomatik kontrol değil, aynı zamanda çevresel farkındalık ve otonomi özellikleriyle ön plana çıkan yeni nesil bir paradigma olarak değerlendirilmektedir (Putnik vd., 2019). Bu sistemler fiziksel alandaki sensör ve cihazlardan gelen verilerin siber alandaki bulut ortamına aktarılması, burada işlenerek kararlara dönüştürülmesi ve tekrar fiziksel ortama müdahale edilmesi biçiminde çift yönlü bir etkileşime dayanır. Bu karşılıklı bağımlılık, CPS'nin çevik, otonom ve adaptif yapısının temelini oluşturur (Agrawal & Kumar, 2022).

ICPS, fiziksel süreçlerin dijital kontrol sistemleriyle entegre edilerek gerçek zamanlı izlenmesini, analizini ve yönetimini sağlayan yapılardır. Bu sistemler, yapay zekâ, IIoT ve otomasyon teknolojileriyle desteklenerek fiziksel ve siber bileşenler arasında karşılıklı veri alışverişini mümkün kılar. ICPS, endüstriyel süreçlerde yüksek düzeyde doğruluk, verimlilik ve esneklik sağlamak amacıyla geliştirilmiş, çok katmanlı

ve etkileşimli sistemlerdir (Jan vd., 2021). Bu çok katmanlı yapı; fiziksel katmanda yer alan IIoT sensörleri, cihazlar ve ağ geçitlerinden elde edilen verilerin, siber katmanda yer alan bulut ortamında işlenmesiyle; uygulama katmanında akıllı robotik, üretim optimizasyonu, arıza süresi azaltımı ve gelişmiş izleme gibi çıktılara dönüştürülmesini sağlamaktadır. Katmanlar arası karşılıklı bağımlılık ve veri akışı, sistemin bütüncül çalışmasını mümkün kılmaktadır (Agrawal & Kumar, 2022).

IoT paradigması, kaynakları sınırlı heterojen cihazlar arasında iletişim sağlamak üzere çeşitli protokollerin ve standartların benimsendiği bir yapı sunmaktadır. Özellikle e-sağlık, akıllı tarım, endüstri 4.0 ve askeri uygulamalar gibi kritik alanlarda kullanılan IoT sistemlerinde, kablosuz iletişimin doğası gereği ihlal riski oldukça yüksektir. Bu durum, siber güvenlik disiplini kapsamında çok katmanlı koruma mekanizmalarını zorunlu kılmaktadır. Dijital dönüşümün hızlanmasıyla birlikte sofistike hale gelen siber tehdit ortamı, gizlilik, bütünlük ve erişilebilirlik prensipleri etrafında şekillenen kapsamlı güvenlik çerçevelerini gerektirmektedir. IoT sistemlerinde bu gereksinimler özelinde; kimlik doğrulama, veri bütünlüğünün korunması, yetkilendirme mekanizmaları ve proaktif risk yönetimi yaklaşımları hayati önem taşımaktadır (Kaur vd., 2023; Lallie vd., 2025; Rizzardi vd., 2022). Modern güvenlik stratejileri, sürekli evrim geçiren tehditlere karşı bu temel unsurları korumayı hedefleyen entegre çözümler üzerine inşa edilmektedir.

Endüstri 4.0 ve dijital dönüşüm süreçlerinin siber güvenlik tehditlerini çeşitlendirmesi ve karmaşıklaştırması nedeniyle, bu artan risklere karşı etkili koruma sağlamak amacıyla çok katmanlı derinlemesine Savunma Derinliği yaklaşımı öne çıkmaktadır. Bu yaklaşım, güvenlik önlemlerini farklı seviyelerde bütüncül bir şekilde uygulayarak sistemleri daha dirençli hale getirir. İlk olarak, politika düzeyinde erişim kontrolü, güncelleme yönetimi ve veri yedekleme gibi konulara yönelik kapsamlı kurallar belirlenirken; süreç seviyesinde ağ güvenlik duvarları, saldırı tespit sistemleri ve kimlik doğrulama mekanizmaları gibi teknik savunma araçları devreye girer. Teknoloji katmanında ise şifreleme, VPN kullanımı, beyaz listeleme ve uç nokta güvenliği gibi yöntemlerle veri ve iletişim güvenliği sağlanır. Bu çok katmanlı yapı sayesinde kuruluşlar, yalnızca belirli tehdit türlerine değil, genel olarak tüm siber saldırı vektörlerine karşı daha dayanıklı hale gelerek sürdürülebilir ve esnek bir savunma hattı oluşturabilirler (Wai & Lee, 2024).

Sıfır Güven Mimarisi (Liu vd., 2024), temel olarak "Hiçbir şeye güvenme, her şeyi doğrula." prensibine dayanan modern bir siber güvenlik yaklaşımıdır. Bu model, geleneksel çevre tabanlı güvenlik anlayışını terk ederek, tüm erişim isteklerinin sürekli doğrulanmasını ve en düşük ayrıcalık ilkesini temel alır. Temel bileşenleri arasında çok faktörlü kimlik doğrulama (MFA), bağlamsal erişim kontrolü, sürekli izleme ve dinamik politika uygulama yer alır. Sıfır Güven, kullanıcıların konumuna bakılmaksızın her erişim girişiminin potansiyel bir tehdit olarak değerlendirilmesini ve veri korumanın şifreleme, segmentasyon gibi yöntemlerle sağlanmasını öngörür. Bu yaklaşım özellikle bulut bilişim, hibrit çalışma modelleri ve IoT cihazlarının yaygınlaştığı günümüz dijital ortamlarında kritik önem taşımaktadır (Dhiman vd., 2024).

Kriptografik sistemler, kullanıcıların hassas verilere erişebilmesi için geçerli kimlik bilgileri (kullanıcı adı, şifre, özel anahtar vb.) sunmasını zorunlu kılarak güvenli erişim sağlar. Bu yöntem, veri korumanın dört temel unsuru olan gizlilik (yetkisiz erişimin engellenmesi), bütünlük (verilerin değiştirilememesi), kimlik doğrulama (kullanıcıların tanımlanması) ve inkar edilemezlik (işlemlerin kayıt altına alınması) ilkelerini destekler. Modern kriptografi teknikleri, güvenilir olmayan ağ ortamlarında bile verilerin güvenli şekilde iletilmesini ve saklanmasını mümkün kılarak, dijital iletişimin güvenilirliğini ve dayanıklılığını artırır. Özellikle asimetrik şifreleme yöntemleri, güçlü kimlik doğrulama mekanizmaları sunarak yetkisiz erişim girişimlerini engellemede kritik rol oynar (Shivam vd., 2022).

CPS ve ICS için siber güvenlik, fiziksel süreçler ve güvenlik üzerindeki potansiyel etkiler nedeniyle kritik öneme sahiptir. Bu zorlukları ele almak için çeşitli standartlar ve çerçeveler geliştirilmiştir. Örneğin, IEC 62443 serisi, endüstriyel otomasyon ve kontrol sistemlerinin güvenliği için kapsamlı bir standart seti sunar ve terminolojiden teknik güvenlik gerekliliklerine kadar geniş bir yelpazeyi kapsar (Leander vd., 2019; Culot vd., 2021). NIST Özel Yayını 800-82, SCADA sistemleri de dahil olmak üzere ICS'nin güvenliğini sağlamak için rehberlik sunar (Stouffer vd., 2015). Ayrıca, ISO/IEC 27001 (Culot vd., 2021), genel bilgi güvenliği yönetim sistemleri standardı olarak, CPS'nin özel ihtiyaçlarına uyarlanabilir (Bicaku vd., 2019). Gelişmiş güvenlik kavramları olarak savunma derinliği ve sıfır güven mimarisi, endüstriyel sistemlerin güvenlik duruşunu artırmak için uygulanmaktadır.

CPS risk değerlendirme ve tehdit modelleme, sistemlerin hem siber hem de fiziksel katmanlarını dikkate alarak güvenlik açıklarını sistematik bir şekilde tanımlamak için kritik bir öneme sahiptir. STRIDE modeli, sahtecilik, veri değiştirme, inkar, bilgi ifşası, DoS ve ayrıcalık yükseltme gibi tehditleri belirlemek için CPS ortamlarında yaygın olarak kullanılmaktadır (Saßnick vd., 2024). Örneğin, mikro şebeke sistemlerinde STRIDE'ın uygulanması, tehditlerin sistematik olarak sınıflandırılmasını ve önceliklendirilmesini sağlamıştır (Khalil vd., 2023). Bu model, CPS'nin karmaşık yapısında tehdit analizini yapılandırmak için etkili bir çerçeve sunar. Ayrıca, DREAD modeli, tehditlerin ciddiyetini değerlendirmek ve risk önceliklendirme süreçlerini desteklemek amacıyla CPS bağlamında, özellikle de ICS'te risk analizinde yaygın olarak kullanılmaktadır (Kavallieratos vd., 2022).

NIST Risk Yönetim Çerçevesi (RMF) ve ISO/IEC 27005 gibi standartlar, CPS ve IoT sistemlerinde risk yönetimini yapılandırılmış bir şekilde ele almak için rehberlik sağlar. NIST RMF, CPS'nin siber ve fiziksel bileşenlerini kapsayan esnek bir risk yönetimi süreci sunarken, ISO/IEC 27005, özellikle IoT cihazlarının heterojen yapısından kaynaklanan risklerin değerlendirilmesine odaklanır (Griffor vd., 2017; ISO/IEC, 2022). Bu standartlar, Endüstri 4.0 ve SCADA sistemlerinde proaktif risk yönetimi için temel oluşturur. Ancak, CPS'nin gerçek zamanlı gereksinimleri ve siber-fiziksel etkileşimlerin karmaşıklığı, bu yöntemlerin uyarlanmasını gerektirir, bu da gelecekteki araştırmalar için önemli bir odak alanıdır.

Siber saldırılar genellikle üç ana kategoride sınıflandırılır: Erişilebilirlik veya kullanılabilirlik saldırıları, bütünlük saldırıları ve gizlilik saldırıları (Duo vd., 2022). Erişilebilirlik saldırıları, sistemlerin veya hizmetlerin erişilemez hale getirilmesini hedefler, örneğin DoS saldırıları (Maseno vd., 2022). Bütünlük saldırıları, veri veya sistemlerin manipüle edilmesiyle ilgilidir, örneğin yanlış veri enjeksiyonu (false data injection) (Baybulatov & Promyslov, 2021). Gizlilik saldırıları ise yetkisiz erişim veya veri sızıntısını içerir (Lone vd., 2023). Bu kategorilerden gizlilik saldırıları, özellikle yetkisiz erişimle ilişkilidir ve bu bölümün ana odak noktasıdır.

Yetkisiz erişim saldırılarının CPS ve ICS üzerindeki etkilerini anlamak için tarihi örnekler önemlidir. Bu örnekler, yetkisiz erişim saldırılarının yalnızca dijital değil, aynı zamanda fiziksel dünyada da ciddi sonuçlar doğurabileceğini göstermektedir. Örneğin,

Stuxnet, nükleer santrifüjlerin fiziksel olarak hasar görmesine neden olurken, BlackEnergy Ukrayna'da binlerce haneyi elektriksiz bırakmıştır (Miller vd., 2021).

2.2. İlgili Çalışmalar

CPS, fiziksel süreçlerle siber bileşenlerin geri beslemeli biçimde etkileşime girdiği karmaşık sistemlerdir. Bu sistemler; ICS, akıllı şebekeler ve otonom araçlar gibi kritik altyapılarda yaygın şekilde kullanılmaktadır. CPS'lerin güvenliği, yalnızca fiziksel tehditlere değil aynı zamanda gelişmiş siber saldırılara karşı da koruma sağlamayı gerektirdiğinden, geleneksel güvenlik yaklaşımlarından farklı ve daha kapsamlı çözümler gerektirir (Castillo vd., 2023).

Castillo ve arkadaşları (2023), CPS ortamı için yarı denetimli bir otoenkoder mimarisi kullanan ve aykırı değer tespitiyle eşik değerlerini dinamik olarak belirleyen yenilikçi bir izinsiz giriş tespit sistemi olan CPS-GUARD'ı geliştirmiştir. CPS-GUARD, çeşitli sistemlerde yüksek doğruluk (%96.1–99.9), yüksek geri çağırma (%94.9–100) ve düşük yanlış pozitif oranları (%0.6–2.7) elde ederek mevcut yöntemlerle rekabetçi sonuçlar sunmuştur. Benzer şekilde, Mansour (2022), CPS ortamında güvenliği artırmak için blok zincir teknolojisiyle entegre edilmiş ve meta-sezgisel algoritmalarla optimize edilmiş derin öğrenme tabanlı bir izinsiz giriş tespit modeli olan PRO-DLBIDCPS tekniğini önermiştir. Bu modelde, özellikle dikkat mekanizmalı çift yönlü geçitli yinelemeli sinir ağı (ABi-GRNN) kullanılarak saldırıların sınıflandırılması sağlanmış, hiperparametre optimizasyonunda ise Zengin-Fakir Optimizasyon (PRO) algoritması kullanılmıştır. Sonuçlar, yüksek doğruluk ve güçlü saldırı tespit başarımı ile PRO-DLBIDCPS'in etkinliğini ortaya koymuştur.

Bu bağlamda, CPS'lerdeki güvenlik tehditlerine karşı farklı yaklaşımlar da dikkat çekmektedir. Örneğin, Javaheri ve arkadaşları (2023), DDoS saldırılarına odaklanarak, bulanık mantık tabanlı tespit yöntemlerini sistematik bir şekilde incelemişlerdir. Çalışmalarında, DDoS saldırılarının karmaşıklığını ve Endüstri 4.0 döneminde iş sürekliliği için oluşturduğu tehditleri ele almışlar, bulanık mantık tabanlı yöntemlerin mevcut izinsiz giriş tespit sistemlerindeki eksiklikleri gidermede etkili olduğunu belirtmişlerdir. Bu yöntemler, özellikle yüksek doğruluk ve düşük yanlış pozitif

oranlarıyla, CPS'lerdeki karmaşık siber tehditlere karşı güçlü bir savunma stratejisi sunmaktadır.

Öte yandan, IoT cihazlarına yönelik tehditler de CPS güvenliği açısından önemli bir odak noktasıdır. Azimjonov ve Kim (2024), kaynak kısıtlı IoT cihazları için hafif ve yüksek doğruluklu bir izinsiz giriş tespit sistemi önermişlerdir. Bu sistem, stokastik gradyan iniş sınıflandırıcısı (SGDC) ve dört özellik seçimi algoritmasını kullanarak, KDD-CUP-1999, BotIoT-2018 ve N-BaIoT-2021 veri setlerinde ortalama %92.69 doğruluk elde etmiş ve özellik sayısını ortalama %79.93 oranında azaltmıştır. Bu yaklaşım, CPS'lerdeki IoT entegrasyonlarında enerji verimliliği ve tespit doğruluğunu artırmak için önemli bir katkı sunmaktadır.

Ayrıca, federatif öğrenme tabanlı yaklaşımlar da CPS güvenliğinde yenilikçi çözümler sunmaktadır. Huang ve arkadaşları (2023), CPS'lerdeki siber tehditlere karşı kişiselleştirilmiş federated öğrenme temelli bir Yürütme ve Değerlendirme Çift Ağı (EEFED) çerçevesi önermişlerdir. Bu çerçeve, dengesiz ve bağımsız olmayan veri dağıtımlarında model stabilitesini artırarak, yerel tespit modellerinin performansını güçlendirmiş ve çeşitli siber senaryolarda tek model ve mevcut yöntemlerden daha iyi sonuçlar elde etmiştir. Bu yaklaşım, sınırlı saldırı örnekleriyle karşılaşılan durumlarda bile etkili bir çözüm sunmaktadır.

Bunun yanı sıra, CPS'lerdeki DDoS saldırılarına karşı hibrit derin öğrenme modelleri de dikkat çekmektedir. Sharma ve arkadaşları (2023), akıllı sağlık ağları gibi CPS modellerinde DDoS saldırılarını tespit etmek için hafif bir CNN-Çift Yönlü LSTM tabanlı hibrit derin öğrenme modeli önermişlerdir. Bu model, dört evrişimli katman, maksimum havuzlama ve yoğun katmanlar kullanılarak trafik akışlarını iyi huylu ve kötü huylu olarak sınıflandırmış, yüksek doğruluk elde etmiştir. Bu tür hibrit yaklaşımlar, CPS'lerin güvenlik gereksinimlerini karşılamada etkili bir alternatif sunmaktadır.

CPS güvenliğinde hibrit yaklaşımlar da önemli bir yer edinmektedir. Jeffrey ve arkadaşları (2024), CPS'lerde anomali tespiti için imza tabanlı ve eşik tabanlı izinsiz giriş tespit sistemlerini makine öğrenimi tabanlı davranışsal anomali tespitiyle birleştiren bir hibrit model önermişlerdir. Bu model, bilinen tehditlerin hızlı tespitini sağlarken, bilinmeyen tehditlerin daha doğru tespitini mümkün kılmış ve Endüstri 4.0 bağlamında artan saldırı yüzeyine karşı etkili bir çözüm sunmuştur.

Benzer şekilde, Alem ve arkadaşları (2023), Endüstri 4.0 için çift anomali tabanlı bir izinsiz giriş tespit sistemi önermişlerdir. Bu sistem, sinir ağları ve bir karar verme sistemi (DMS) aracılığıyla gerçek saldırıları endüstriyel arızalardan ayırmayı başarmış, yüksek doğruluk ve düşük yanlış pozitif oranlarıyla gerçek endüstriyel ortamlarda umut verici sonuçlar elde etmiştir. Bu yaklaşım, CPS'lerdeki karmaşık tehdit ortamlarında güvenilirlik ve etkinlik açısından önemli bir katkı sağlamaktadır.

Ayrıca, transfer öğrenme tabanlı yöntemler de CPS güvenliğinde dikkat çekmektedir. Saheed ve arkadaşları (2024), CPS'lerde izinsiz giriş tespiti için hafif bir ResNet50-1D-CNN transfer öğrenme modeli önermişlerdir. Bu model, HAI ve UNSW-NB15 veri setlerinde sırasıyla %97.32 ve %99.89 doğruluk oranları elde etmiş, sınırlı etiketli veriyle karşılaşılan durumlarda eğitim ve test sürelerini azaltarak CPS'lerin güvenlik ihtiyaçlarına uygun bir çözüm sunmuştur. Bu tür yaklaşımlar, CPS'lerin kritik altyapılardaki güvenilirliğini artırmada önemli bir rol oynamaktadır.

Benzer şekilde, Liu ve arkadaşları (2024), ağ tabanlı izinsiz girişlerin tespitinde KNN algoritmasını kullanarak eğitim verisinin oluşturulmasında karşılaşılan zorluklara çözüm sunmayı amaçlamıştır. Çalışmada, rastgele yöntemle oluşturulan veri seti ile manuel yöntemle oluşturulan veri setleri karşılaştırılmış; K değeri hem kısmi hem de tüm veri seti üzerinden ayarlanarak model doğruluğu incelenmiştir. Sonuçlar, rastgele yöntemle oluşturulan verilerle elde edilen doğruluk oranlarının manuel yönteme göre daha yüksek olduğunu göstermiştir. CICIDS2017 veri seti kullanılarak yapılan deneyler, önerilen yaklaşımın ağ izinsiz giriş tespitinde etkili olduğunu doğrulamaktadır.

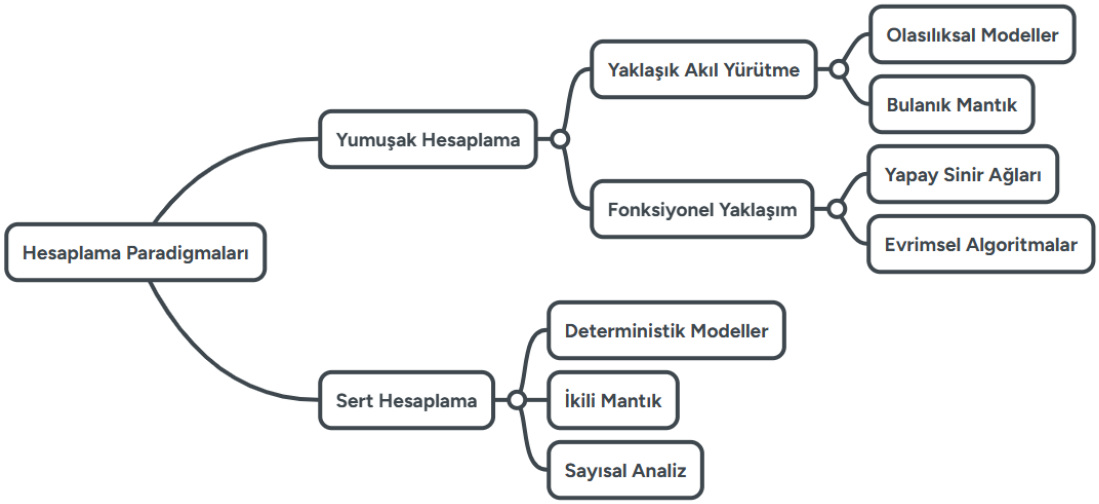
Akıllı şebekeler gibi CPS uygulamalarında da yenilikçi yaklaşımlar öne çıkmaktadır. Ganesan ve Arockia Edwin Xavier (2023), akıllı şebeke ağlarında izinsiz giriş tespiti için olasılıksal yinelemeli sinir ağı (PRNN) sınıflandırıcısına dayalı bir sistem önermişlerdir. Bu sistem, gerçek zamanlı akıllı şebeke verileri ile KDD99 veri setini birleştirerek anomali tespiti gerçekleştirmiş, Geliştirilmiş Aquila Sürü Optimizasyonu (IASO) ile özellik seçimi yaparak yüksek doğruluk, hassasiyet ve tespit oranı elde etmiştir. Ayrıca, Birleşik Güç Kalitesi Denetleyicisi (UPQC) cihazı kullanılarak güç kalitesi iyileştirilmiş ve bulut depolama ile veri yönetimi sağlanmıştır. Bu yaklaşım, akıllı şebekelerin güvenilirliğini ve güvenliğini artırmada etkili bir çözüm sunmaktadır.

Yumuşak hesaplama yöntemleri, CPS'de anormallik tespiti için çeşitli şekillerde uygulanmaktadır. Örneğin, IoT tabanlı sistemlerde anormallik tespiti için MFEW_Bagging adlı bir yöntem geliştirilmiştir. Bu yöntem, hibrit özellik seçimi ve ensemble öğrenme tekniklerini kullanarak normal ve anormal kullanım desenlerini sınıflandırmakta ve gerçek zamanlı kötüye kullanımı önlemektedir (Bhatia & Sangwan, 2024). Çalışma, halka açık bir IDS veri seti üzerinde değerlendirilmiş ve yüksek doğruluk oranları elde edilmiştir.

Son olarak, Yaacoub ve arkadaşları (2020), CPS'de savunma derinliğinin uygulanmasını tartışırken, son araştırmalar CPS için özelleştirilmiş sıfır güven mimarilerini keşfetmektedir. Özellikle, Feng ve Hu (2023), ICPS için tasarlanmış Siber-Fiziksel-ZTA mimarisini önermekte, çok katmanlı erişim kontrol motoru ve entegre fiziksel model tabanlı ile veri odaklı politika iyileştirici gibi yenilikçi tekniklerle sahte veri enjeksiyonu (FDI) saldırılarına karşı tespit olasılığını %31 oranında artıran bir yaklaşım sunmaktadır. Bu standartlar ve yaklaşımlar, kritik altyapıyı korumak ve CPS operasyonlarının güvenilirliğini ve güvenliğini sağlamak için hayati öneme sahiptir.

2.3. Hesaplama Paradigmaları

Makine zekâsı (Rudas, 2003), günümüz bilim ve teknoloji alanlarında giderek önem kazanan disiplinlerarası bir araştırma alanı olarak öne çıkmaktadır. Bu alan, otomatik sistemlerin algılama, tanıma, akıl yürütme ve karar verme gibi bilişsel süreçlerde insan zekâsına benzer veya onu aşan yetkinlikler sergilemesini mümkün kılmaktadır (He & Shen, 2025). Makine zekâsının temelini oluşturan hesaplama paradigmaları, Şekil 2.1'de sistematik olarak sınıflandırılmıştır.



Şekil 2.1. Hesaplama paradigmalarının sınıflandırılması (Falcone vd., 2020)

Sert hesaplamanın sayısal kesinliği ile yumuşak hesaplamanın adaptif öğrenme yeteneği, modern makine zekâsı uygulamalarında sinerjik bir şekilde kullanılmaktadır (Tavana & Sorooshian, 2024). Özellikle yumuşak hesaplama teknikleri (bulanık mantık, yapay sinir ağları ve evrimsel algoritmalar), karmaşık ve belirsiz problemlerin çözümünde insan benzeri esneklik sunmaktadır.

Bu bağlamda, yapay zekâ, çevresel koşullara uygun biçimde tepki verebilen, bu koşullara göre davranışlarını uyarlayabilen ve insan zekâsı gerektirdiği düşünülen görevleri yerine getirebilen sistemlerin geliştirilmesi süreci olarak tanımlanmaktadır (Dix, 2025). Bu esneklik, yapay zekânın geniş bir uygulama yelpazesinde etkili olmasını sağlamaktadır.

Örneğin, uzman sistemler (Aronson, 2003), belirli bir alanda insan uzmanlarının bilgi ve karar alma yeteneklerini taklit eden yazılımlar olarak makine zekâsı kapsamında önemli bir yere sahiptir. Bu sistemler, genellikle eğer-ise kurallarına dayalı bir bilgi tabanından faydalanarak, belirli bir problem alanında uzman düzeyinde çözümler üretir. Elektrik üretim, dağıtım ve iletim sistemleri gibi teknik alanlarda, uzman sistemler parametrelerin hesaplanması ve karar süreçlerinin otomasyonu için etkin bir şekilde kullanılmaktadır. Ancak, bu sistemlerin esnekliği, modern yapay zekâ yaklaşımlarına kıyasla sınırlıdır ve yeni ya da beklenmedik problemlerle karşılaştıklarında uyarlanabilirlikleri kısıtlıdır. Buna rağmen, uzman sistemlerin geliştirilmesi ve bakımı,

karmaşık öğrenme modellerine göre daha kolay ve maliyet-etkindir, bu da onları belirli uygulamalarda tercih edilebilir kılmaktadır (Sajid vd., 2023).

Bu noktada, Lütfi Aliasker Zade'nin öncülük ettiği yaklaşım (Zadeh, 1994), makine zekâsını sert hesaplama ve yumuşak hesaplama teknikleri üzerinden farklı perspektiflerle ele almaktadır. Sert hesaplama paradigması, kesin matematiksel modellere ve deterministik algoritmalara dayanırken; yumuşak hesaplama, belirsizlik ve yaklaşıklık ilkeleri üzerine kurulu esnek bir çerçeve sunmaktadır (Siddique & Adeli, 2013). Bu çerçevede, yaklaşık akıl yürütme, belirsiz ve eksik bilgiler altında mantıksal çıkarım yapabilmeyi sağlayan, özellikle bulanık mantık ve olasılıksal yaklaşımları temel alan bir akıl yürütme metodolojisidir (Aliev vd., 2024).

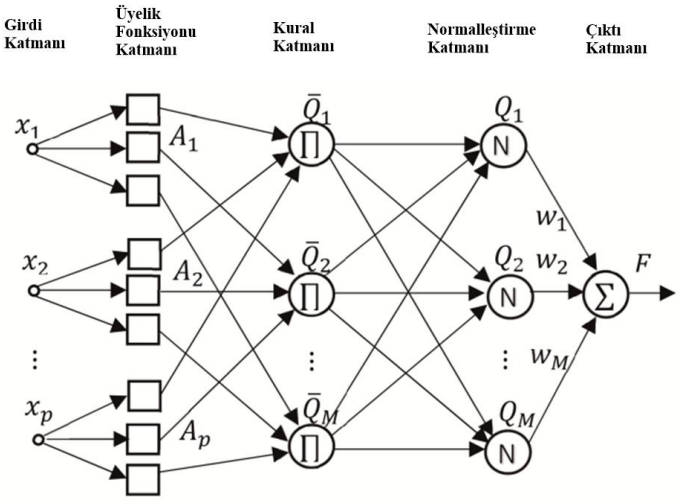
Benzer şekilde, sezgi üstü algoritmalar, karmaşık optimizasyon problemlerini çözmek için hesaplama zekâsına dayalı güçlü bir yaklaşım sunar. Bu algoritmalar, rasgele örnekleme tabanlı yöntemleri yönlendirilmiş arama stratejileriyle birleştirerek, arama uzayında en uygun veya ona yakın bir çözümü bulmayı hedefler. Keşif ve sömürü aşamalarını dengeleyerek optimizasyon sürecini etkinleştiren bu yöntemler, genellikle deneme-yanılma yoluyla tekrarlayan hesaplama görevlerinden oluşur. Örneğin, Genetik Algoritma'da mutasyon aşaması arama uzayının farklı bölgelerine yerleşimi sağlarken, çaprazlama aşaması komşu bölgelerde daha iyi çözümlere yönelir. Benzer şekilde, Emperyalist Rekabet Algoritması'nda devrim eylemi arama uzayında çeşitliliği artırırken, asimilasyon politikası daha iyi çözümlere doğru hareketi sağlar. Bu süreçlerde, genellikle uniform dağılımlar yerine Normal veya Cauchy gibi olasılıksal dağılımların kullanılması, arama uzayında daha iyi çeşitlilik sağlar. Bununla birlikte, rasgele seçimlerin belirsizliği nedeniyle, kaos haritalarının deterministik ve doğrusal olmayan davranışlarından faydalanılması, yerel optimumlara takılmayı önleyerek küresel çözümlere yönelimi güçlendirir. Kaos serileri, özellikle doğrusal olmayan ve dışbükey olmayan hedef fonksiyonların optimizasyonunda, örneğin kafes ağırlık optimizasyonunda, algoritmaların erken yakınsama sorununu azaltarak performansı artırır. Dolayısıla, sezgi üstü algoritmalar, evrimsel algoritmalar, yapay sinir ağları ve bulanık mantık gibi yumuşak hesaplama teknikleriyle sinerji oluşturarak, yüksek boyutlu, süreksiz veya türev alınamayan problemlerde insan benzeri esneklik sağlar (Zolghadr-Asli, 2023; Kaveh & Yousefpoor, 2024).

Sonuç olarak, bu bölümde, makine zekâsının gelişiminde kritik rol oynayan hesaplama paradigmaları, teorik temelleri ve pratik uygulamalarıyla birlikte ele alınmıştır. Detaylı algoritmik formülasyonlar ve uygulama örnekleri, çalışmanın 3. Materyal ve Yöntem bölümünde sunulacaktır.

2.3.1. Bulanık Mantık ve Uyarlamalı Nöro-Bulanık Çıkarım Sistemi (ANFIS)

Bulanık mantık, klasik (iki değerli) mantığın kesin sınırlarına alternatif olarak geliştirilmiş bir yaklaşımdır. Klasik mantıkta her önerme ya doğru (1) ya da yanlış (0) olarak değerlendirilirken, bulanık mantıkta doğruluk dereceleri 0 ile 1 arasında sürekli bir değer aralığında tanımlanır. Bu yapı, gerçek dünyadaki belirsizlikleri, gri alanları ve keskin olmayan sınırları matematiksel olarak ifade etmeyi mümkün kılar. İlk olarak Lotfi A. Zadeh tarafından ortaya atılan bulanık mantık, geleneksel mantığın "üçüncü halin imkânsızlığı" ilkesini sorgulayarak, sınıfların net sınırlarla ayrılmadığı durumları da kapsayacak şekilde genişletilmiştir (Tabakov, 2022). Bu bağlamda, bulanık mantık yalnızca teorik matematikte değil, aynı zamanda kontrol sistemleri, yapay zekâ, karar verme süreçleri ve otomasyon teknolojileri gibi birçok uygulama alanında etkin biçimde kullanılmaktadır. Bulanık cebirsel yapılar ve bu yapıların genişletilmiş hâli olan Smarandache bulanık cebiri ise, klasik cebirsel sistemlerin esnek ve gerçek yaşamla daha uyumlu biçimlere dönüştürülmesine imkân tanımaktadır (Tabakov, 2022).

ANFIS, yapay sinir ağları ile Takagi-Sugeno bulanık çıkarım sisteminin birleşiminden oluşan, karmaşık ve doğrusal olmayan sistemleri modellemek için güçlü bir hibrit yaklaşımdır. ANFIS, bulanık mantığın belirsizlik yönetimi ile sinir ağlarının öğrenme ve uyarlama yeteneklerini birleştirerek evrensel bir tahmin aracı olarak öne çıkar. Beş katmanlı mimarisi (Şekil 2.2), üyelik derecelerinin hesaplandığı bulanıklaştırma katmanı, kural ateşleme güçlerini üreten kural katmanı, bu güçleri normalleştiren katman, bulanıklık giderme değerlerini sağlayan katman ve nihai çıktıyı veren katmandan oluşur (Sood vd., 2024; Voloşencu, 2024).



Şekil 2.2. ANFIS modeli yapısı

Genetik algoritmalar, diferansiyel evrim ve parçacık sürü optimizasyonu gibi sezgi üstü yöntemlerle desteklenen ANFIS, çeşitli disiplinlerde modelleme, tahmin ve kontrol sistemlerinde etkin bir şekilde kullanılmaktadır (Voloşencu, 2024).

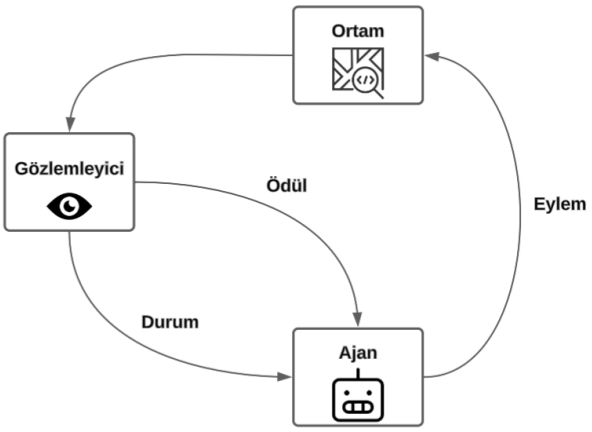
2.3.2. Genetik Algoritmalar (GA)

GA, evrimsel hesaplama alanının temel yöntemlerinden biri olup, doğal seçilim ve genetik süreçlerden esinlenerek yüksek boyutlu ve karmaşık arama–optimizasyon problemlerine etkili çözümler sunan sezgisel algoritmalardır. Charles Darwin'in "en uygun olanın hayatta kalması" ilkesine dayanan bu algoritmalar (Wirsansky, 2024), her bireyin genetik özelliklerini temsil eden gen dizilerini kullanarak çözüm uzayındaki potansiyel çözümleri değerlendirir. Uygunluk değeri ile ölçülen bu bireyler, doğal seçilimi taklit eden bir süreçte çaprazlama ve mutasyon işlemlerine tabi tutularak yeni bireyler üretir ve bu sayede popülasyon, zamanla daha iyi çözümlere evrilir. Olasılıksal yaklaşımla çalışan GA'lar, çözüm uzayında yüksek performanslı bölgeleri hedefleyerek esnek ve güçlü optimizasyon olanakları sunar (Kumar vd., 2024; Lanham, 2023).

2.3.3. Pekiştirmeli Öğrenme (RL) ve Derin Q Ağı (DQN)

RL, Markov karar süreçleri (MDP) çerçevesinde, bir ajanın kısmen rastgele ve kısmen kontrol edilebilen sonuçlarla karşılaştığı durumlarda karar verme süreçlerini

optimize etmeyi amaçlayan bir makine öğrenmesi yöntemidir (Hua, 2024). Bu süreç, Şekil 2.3 ile görselleştirilmiştir.



Şekil 2.3. Pekiştirmeli öğrenme çevrimi

RL algoritmaları, gelecekteki ödülleri maksimize eden "optimal" politikaları öğrenmeyi hedefler. Bu süreç, ayrık durum uzaylarında ve sınırlı sayıda sonuçla çalışıldığında, Markov sürecinin hafızasız özelliği sayesinde çözülebilir hale gelir. Optimal politika, Bellman denklemiyle (Eşitlik 2.1) ifade edilen Q-değer fonksiyonu aracılığıyla, anlık ödül ile gelecekteki indirimli ödüllerin toplamını tahmin ederek belirlenir (Hua, 2024).

$$L(\theta) = E\left(R_t + \gamma max_{a'} Q^{\pi}(S_{t+1}, a' | S_t = s, a; \theta) - Q(S_t, A_t; \theta)\right)^2 \quad (2.1)$$

Derin pekiştirmeli öğrenmede, örneğin Derin Q-Ağları (DQN), Q-değerlerini yaklaşık olarak hesaplamak için derin sinir ağlarını kullanır ve durumları giriş olarak alarak olası eylemler için Q-değerlerini üretir. Eğitim, mevcut Q-değeri tahmini ile hedef Q-değeri arasındaki farkı minimize eden bir kayıp fonksiyonu (genellikle ortalama kare hata) üzerinden gerçekleştirilir. DQN, ana ağ ve hedef ağ ayrımıyla eğitimi stabilize ederken, deneyim tekrar belleği gibi teknikler öğrenme sürecini daha verimli ve kararlı hale getirir (Hua, 2024).

Pekiştirmeli öğrenme, bir ajanın çevresiyle etkileşime girerek ödülünü maksimize edecek en iyi stratejiyi öğrenmesini amaçlar. Derin Q Ağı (DQN) ise bu süreci, deneyim tekrarını ve sabit hedef ağları kullanarak daha verimli ve kararlı hale getiren bir yapay sinir ağı yaklaşımıdır (Li vd., 2022).

Derin Q-öğrenmesi (Deep Q-Learning, DQL), karmaşık optimizasyon problemlerinde Q-değerlerini yaklaşık olarak hesaplamak için derin sinir ağlarını (DNN) kullanan güçlü bir pekiştirmeli öğrenme yöntemidir. Yüksek boyutlu durum uzaylarında ve doğrusal olmayan ilişkilerde etkin olan DQL, deneyim tekrar belleği (replay buffer) kullanarak ajanın çevreyle etkileşimlerinden elde ettiği deneyimleri depolar ve rastgele örnekleme yoluyla bu deneyimlerden öğrenir. Bu, ardışık deneyimlerin korelasyonunu azaltarak öğrenme sürecini daha kararlı hale getirir ve nadir olaylardan öğrenmeyi mümkün kılar. DQL, Q-değerlerini tahmin etmek için kayıp fonksiyonunu minimize eder ve ϵ-greedy gibi keşif-sömürü dengesi stratejileriyle eylemleri seçer. Geleneksel DQL'nin performansını artırmak için çift Q-öğrenmesi, ikili ağ mimarisi, öncelikli deneyim tekrarı, dağılımsal öğrenme, gürültülü ağlar ve çok adımlı öğrenme gibi yenilikler önerilmiştir. Örneğin, çift Q-öğrenmesi aşırı tahmin önyargısını azaltırken, ikili ağ mimarisi durum değerlerini ve eylem beklentilerini ayırarak öğrenme verimliliğini artırır. Bu gelişmeler, DQL'nin örnek verimliliği, kararlılık ve belirsizliğe karşı robustluk gibi zorluklarını ele alarak, özellikle oyun teorisi ve karmaşık kontrol görevlerinde üstün performans sağlar (Faisal vd., 2024).

2.3.4. Karar Ağaçları

Karar ağaçları, bilgiyi yapılandırılmış bir biçimde temsil etmek, sınıflandırma yapmak ve çeşitli karar verme problemlerini çözmek amacıyla kullanılan hiyerarşik yapılardır. Özellikle bilgi temsili, kombinatoryal optimizasyon ve hesaplamalı geometri gibi alanlarda yaygın olarak kullanılan karar ağaçları, hem teorik hem de uygulamalı yapay zekâ çalışmalarında önemli bir yer tutar. Bu ağaç yapıları, özniteliklere dayalı sorgularla adım adım ilerleyerek bir karara ulaşır ve bu yönüyle test teorisi, kaba küme teorisi ve kesin öğrenme gibi öğrenme modelleriyle de doğrudan ilişkilidir. Geleneksel karar ağaçlarının yanı sıra, hipotez içeren modellerin de kullanımıyla daha düşük karmaşıklıkla daha etkili sınıflandırmalar yapılabilmekte, böylece karar ağaçları sadece

sınıflandırma değil, bilgi temsili ve Boole fonksiyonlarının hesaplanmasında da güçlü araçlar hâline gelmektedir (Azad vd., 2022).

2.3.5. Doğrusal Diskriminant Analizi (LDA)

Doğrusal Diskriminant Analizi (LDA), özellikle sınıflar arasındaki ayrımı en iyi şekilde gerçekleştirmek amacıyla kullanılan denetimli bir boyut indirgeme yöntemidir. LDA, veri kümesindeki sınıflar arasındaki farkı en üst düzeye çıkarırken, aynı sınıf içindeki örneklerin benzerliğini korumaya çalışır. Böylece, yüksek boyutlu veriler daha az boyutlu fakat daha ayrıştırıcı bir alt uzaya dönüştürülür. Bu yöntem, sınıflandırma algoritmalarının hem eğitim süresini azaltır hem de sınıf ayrımını daha belirgin hale getirerek yorumlanabilirliği artırır. Genellikle tek bir dönüşüm matrisi kullanılarak tüm sınıflar aynı boyut indirgeme sürecinden geçirilir, bu da yöntemlerin sınıf bağımsız (class-independent) biçimde uygulanmasına olanak tanır (Pradhan, 2023).

2.3.6. Lojistik Regresyon

Lojistik regresyon, sınıflandırma problemleri için geliştirilmiş olup, doğrusal bir değeri sigmoid fonksiyonla 0 ile 1 arasında bir olasılığa dönüştürerek sınıf tahmini yapar; buna karşılık doğrusal regresyon, bağımlı değişkenin sürekli olduğu durumlarda bağımsız değişkenlerin etkisini doğrusal bir denklemle modelleyerek parametre tahminleri en küçük kareler yöntemiyle yapılır. Her iki yöntem de bağımsız değişkenlerin etkilerini analiz etmek için güçlü istatistiksel araçlar olmakla birlikte, lojistik regresyonda katsayıların yorumlanabilirliği ve karşılaştırılabilirliği açısından bazı sınırlamalar bulunmaktadır (Salerno, 2025; Hagenaars vd., 2025).

2.3.7. Naive Bayes

Naive Bayes sınıflandırıcısı, Bayes teoremi temel alınarak geliştirilen, olasılık temelli ve denetimli bir makine öğrenmesi yöntemidir. Bu yöntem, sınıflandırma problemlerinde, önceden bilinen olasılıkları ve gözlemlenen verileri kullanarak bir olayın gerçekleşme ihtimalini hesaplar. Naive Bayes, büyük veri kümelerini hızlı ve basit şekilde sınıflandırabilmesi sayesinde özellikle duygu analizi, metin sınıflandırma, istenmeyen e-posta filtresi ve öneri sistemlerinde yaygın olarak kullanılır. Hesaplama açısından oldukça verimli olması nedeniyle, veri miktarının az olduğu durumlarda daha karmaşık modellere kıyasla üstün performans gösterebilir (N. V. Jagan Mohan vd., 2024).

2.3.8. Destek Vektör Makineleri (SVM)

SVM, denetimli öğrenme yöntemleri arasında yer alır ve genellikle sınıflandırma ile regresyon problemlerinde kullanılır. Algoritma, veri noktalarını n boyutlu bir uzayda konumlandırarak, sınıfları ayıran en uygun hiper düzlemi belirlemeye çalışır. Veriler doğrusal olarak ayrılamadığında ise çekirdek fonksiyonu devreye girer ve veriler daha yüksek boyutlu bir uzaya taşınarak ayrılabilir hale getirilir. Karar sınırına en yakın olan ve sınıflandırmayı etkileyen veri noktalarına destek vektörleri denir; bu noktalar kullanılarak sınıflandırıcı marjini maksimize eder ve böylece modelin genel performansı yükseltilir (Anoop V.S vd., 2025).

2.3.9. K-En Yakın Komşu (KNN)

KNN algoritması, denetimli ve parametre gerektirmeyen bir makine öğrenimi yaklaşımı olarak sınıflandırma ve regresyon görevlerinde yaygın şekilde kullanılmaktadır. Bu algoritma, yeni bir veri örneğini sınıflandırmak için, eğitim veri kümesindeki örneklerle olan benzerlik derecesini değerlendirir ve sınıflandırma işlemini, en yakın k komşunun sınıf etiketlerine göre gerçekleştirir. Benzerlik değerlendirmesi genellikle Öklidyen mesafeye dayalı olarak yapılır; böylece yeni veri noktası, örüntülerin en çok benzediği sınıfa atanır. KNN algoritması, eğitim aşamasında verileri yalnızca depoladığı için eğitim süreci oldukça hızlıdır; ancak sınıflandırma sırasında tüm veri kümesiyle mesafe hesaplaması yaptığı için hesaplama yükü tahmin aşamasında ortaya çıkar. K parametresi, kararın kaç komşuya göre verileceğini belirleyen temel unsurdur ve modelin duyarlılığı üzerinde doğrudan etkilidir (Siddique vd., 2023; Adjei vd., 2024).

2.3.10. Evrişimli Sinirsel Ağ (CNN) Algoritması

CNN, derin öğrenmede sıkça kullanılan yapılar olup evrişimsel katmanlar, havuzlama katmanları, doğrusal olmayan birimler, tam bağlantılı katmanlar ve bazı durumlarda toplu normalizasyon gibi yapı taşlarından oluşur. Girdi katmanı sabit boyutlu veriyi alırken, evrişimsel katman filtreler yardımıyla önemli özellikleri çıkarır ve uzamsal ilişkileri korur. Bu katmanı genellikle döngüsel olarak kullanılan bir havuzlama katmanı izler; havuzlama işlemi, özellik haritalarının boyutunu küçülterek hesaplama maliyetini düşürür. Ardından gelen tam bağlantılı katmanlar sınıflandırmayı gerçekleştirirken, bazı durumlarda bu katmanların yerine küresel düz havuzlama tercih edilir. Ayrıca, aşırı

uyumu önlemek için dropout uygulanabilir. CNN'lerde kullanılan aktivasyon fonksiyonları modelin doğrusal olmayan ilişkileri öğrenmesini sağlar; ReLU hızlı ve yaygın kullanılan bir seçenekken, sigmoid ikili sınıflandırmalarda, softmax ise çok sınıflı problemlerde olasılık dağılımı sağlamak amacıyla kullanılır. Bu katmanlar ve tekniklerle CNN'ler, karmaşık veri yapılarından otomatik olarak anlamlı özellikler çıkararak yüksek doğrulukta sonuçlar elde edilmesini sağlar (Kanagachidambaresan & Bharathi, 2024; Kumar vd., 2025).

2.3.11. Uzun Kısa Dönemli Bellek (LSTM) Algoritması

LSTM ağları, klasik yinelemeli sinir ağı (RNN) mimarisinin zamanla azalan bellek etkisini ve uzun vadeli bağımlılıkları öğrenme konusundaki yetersizliğini aşmak amacıyla geliştirilmiş özel bir yapıdır. Geleneksel RNN'ler yalnızca bir önceki adımın çıktısına erişebildiği için kısa vadeli belleğe sahiptir ve bu durum, uzun veri dizileri içindeki uzak ilişkilerin öğrenilmesini zorlaştırır. LSTM mimarisi ise, bu sınırlamayı aşmak ve bilginin daha uzun süre korunmasını sağlamak amacıyla unutma kapısı, giriş kapısı ve çıkış kapısı olmak üzere üç temel bileşen içerir. Bu kapılar, bilginin hangi kısmının korunacağına, güncelleneceğine veya dışa aktarılacağına karar verilmesini sağlar. Unutma kapısı, geçmiş bilgilerden hangilerinin silineceğini belirlerken; giriş kapısı, yeni gelen bilginin hangi kısmının hücre durumuna ekleneceğini saptar; çıkış kapısı ise hücrede tutulan bilginin ne kadarının bir sonraki katmana aktarılacağını kontrol eder. Bu yapı sayesinde LSTM ağları, uzun süreli bağımlılıkları öğrenme yeteneğine sahip olurken aynı zamanda belleği verimli bir şekilde kullanır. Ancak bu avantajları, klasik RNN'lere kıyasla daha fazla hesaplama karmaşıklığı getirmektedir (Vishwas & Macharla, 2025; Jentzen vd., 2025).

2.4. Gerçek Veri Setlerinin Toplanması ve Seçilmesi

Bu çalışmada CSE-CIC-IDS2018, CIC-ToN-IoT ve Edge-IIoTset veri kümelerinin tercih edilmesinin temel nedeni, bu veri setlerinin hem güncel saldırı türlerini hem de farklı ağ ve sistem altyapılarını temsil etme yeteneğidir. CSE-CIC-IDS2018, geleneksel ağlar üzerinde gerçekleştirilen çeşitli saldırı senaryolarını kapsayarak klasik NIDS modelleri için güçlü bir test ortamı sunarken, CIC-ToN-IoT veri kümesi ise IoT ortamlarında karşılaşılan güvenlik tehditlerine odaklanmakta ve çok sınıflı etiketleme yapısıyla ayrıntılı saldırı analizi yapmaya olanak tanımaktadır. Bu iki veri kümesi, ortak

bir format olan CICFlowMeter ile işlenmiş olup, özellik tutarlılığı sayesinde farklı modellerin karşılaştırmalı olarak değerlendirilmesine imkân sağlamaktadır. Öte yandan, Edge-IIoTset veri seti, gerçek dünya IIoT sistemlerini simüle eden çok katmanlı bir altyapıya ve çeşitli cihazlara yönelik saldırıları içermesiyle siber fiziksel sistemlerin güvenlik analizinde kritik bir rol üstlenmektedir. Ayrıca, bu veri seti ağ trafiği, sistem kaynakları ve log bilgilerini bir araya getirerek yalnızca ağ düzeyinde değil, sistemsel düzeyde de saldırıların izlenmesini ve tespit edilmesini mümkün kılmaktadır. Tüm bu veri setleri, farklı saldırı tipleri, sistem ortamları ve veri kaynaklarını içermesi sayesinde model genellenebilirliğinin sağlanması ve çok yönlü savunma mekanizmalarının geliştirilmesi açısından ideal bir temel sunmaktadır.

CSE-CIC-IDS-2018 ve CIC-ToN-IoT veri kümeleri, makine öğrenimi tabanlı Ağ Saldırı Tespit Sistemlerinin (NIDS) performansını değerlendirmek amacıyla yaygın şekilde kullanılan, farklı ağ ortamlarından ve saldırı senaryolarından elde edilmiş kapsamlı veri setleridir. CSE-CIC-IDS-2018 veri kümesi, siber saldırı tespitine yönelik araştırmaların gelişimine katkı sağlayan en güncel veri setlerinden biridir. 14 farklı saldırı türünü içeren büyük ve herkese açık bir yapıya sahip olması, makine öğrenimi modellerinin eğitimi açısından uygun hale getirirken, boyutu ve çeşitliliği nedeniyle bazı zorlukları da beraberinde getirmektedir (Hewapathirana, 2025). CICFlowMeter aracıyla oluşturulmuş bu veri kümesi, ayrıntılı ağ akışı özellikleri sunmaktadır. Öte yandan, IoT altyapılarına yönelik saldırıları içeren ve son dönemde yaygın şekilde benimsenen en güncel veri kümelerinden biri olan CIC-ToN-IoT, ToN-IoT veri kümesinin CICFlowMeter formatına dönüştürülmesiyle elde edilmiş olup, ikili ve çok sınıflı etiketleme yapısıyla farklı saldırı türlerinin ayrıştırılmasını kolaylaştırmaktadır (Talpini vd., 2023). Bu veri kümeleri, NetFlow ve CICFlowMeter gibi ortak özellik setlerine dönüştürülerek, farklı modellerin tespit performanslarını karşılaştırmalı şekilde değerlendirme imkânı sunmakta ve böylece modellerin genellenebilirliğini test etme açısından önemli bir rol oynamaktadır. Bu sayede, hem farklı saldırı türlerinin tanınmasında daha güvenilir sonuçlar elde edilmekte hem de akademik araştırmaların pratik uygulamalara entegrasyonu kolaylaştırılmaktadır (Sarhan vd., 2022).

Edge-IIoTset (Ferrag vd., 2022), çeşitli endüstriyel IoT cihazlarıyla ilişkili saldırı türlerini kapsayan kapsamlı bir veri kümesidir. Toplamda on farklı cihaz türü (örneğin, ultrasonik sensörler, pH ölçerler, su seviyesi ve nem izleyicileri) içeren bu veri seti, 13

farklı saldırı sınıfını beş temel tehdit başlığı altında toplamaktadır: adam-ortadaki saldırılar, DoS/DDoS, bilgi toplama, zararlı yazılım ve enjeksiyon saldırıları. 1176 özellikten seçilen 61 nitelik, ağ trafiği, sistem kaynakları ve loglar gibi farklı kaynaklardan elde edilmiş olup yüksek korelasyona sahiptir. Test ortamı yedi katmandan oluşmakta (örneğin, uç bilişim, blokzincir ağı, bulut bilişim) ve veri ön işleme aşamalarında eksik veri temizliği, yinelenen kayıtların kaldırılması ve kategorik değişkenlerin dönüştürülmesi gibi adımlar uygulanmıştır (Singh & Chauhan, 2024).

Çalışmada tek bir veri seti yerine üç farklı veri setinin seçilmesinin temel nedeni, farklı ağ ve sistem ortamlarını kapsayarak modelin genellenebilirlik ve sağlamlığını artırmaktır. CSE-CIC-IDS2018 veri seti, daha çok genel ağ ortamlarında gerçekleşen siber saldırıları içerirken; CIC-ToN-IoT, özellikle IoT cihazlarına yönelik tehditlere odaklanmaktadır. Buna karşın, Edge-IIoTset veri kümesi ise endüstriyel IoT ve siber fiziksel sistemlerdeki karmaşık ve çok katmanlı saldırı senaryolarını temsil etmektedir. Böylece, üç farklı veri setiyle yapılan değerlendirme, yalnızca tek bir ortamda değil, genel ağlardan IoT ve endüstriyel sistemlere kadar geniş bir yelpazede modelin performansını ölçmeye olanak tanımaktadır. Bu yaklaşım, geliştirilen yöntemlerin farklı kullanım alanlarında etkinliğini ve güvenilirliğini ortaya koymak adına kritik öneme sahiptir.

BÖLÜM 3

3. MATERYAL ve YÖNTEM

3.1. Yöntemlerin Matematiksel Modelleri

Bu bölümde, saldırı tespitine yönelik kullanılan yapay zekâ ve yumuşak hesaplama yöntemlerinin matematiksel temelleri açıklanmıştır. Öncelikle modellerin kategorilere ayrılması ve literatürdeki referanslara göre konumlandırılması yapılmış, ardından çalışmada detaylı olarak uygulanan modellere ait algoritmik yapı ve denklemler sunulmuştur.

3.1.1. Bulanık Mantık

Bulanık mantık sistemleri, belirsizlik içeren çok değişkenli problemlerin modellenmesinde yaygın olarak kullanılmaktadır. Bu sistemlerin temelinde, klasik küme teorisinin genişletilmiş bir versiyonu olan bulanık küme teorisi yer almaktadır. Bulanık küme teorisine göre, bir $\tilde{A}$ bulanık kümesi, tanım kümesi X üzerinde tanımlı sürekli bir üyelik fonksiyonu ile ifade edilir (Denklem 3.1):

$$\tilde{A} = \{(x, \mu_{\tilde{A}}(x)) \mid x \in X, \mu_{\tilde{A}}(x) \in [0,1]] \} \tag{3.1}$$

Burada $\mu_{\tilde{A}}(x)$, x öğesinin $\tilde{A}$ kümesine aitlik derecesini belirtir.

Klasik giriş değişkeni x, uygun bir üyelik fonksiyonu ile bulanık değişkene dönüştürülür (Denklem 3.2):

$$x \to \mu_{\tilde{A}}(x) \tag{3.2}$$

Üyelik fonksiyonları genellikle üçgen, yamuk veya Gauss dağılımı gibi şekillerde tanımlanır. Örneğin, üçgensel bir üyelik fonksiyonu aşağıdaki gibi tanımlanır (Denklem 3.3):

$$\mu(x) = \begin{cases} 0, & x \leq a \\ \dfrac{x-a}{b-a}, & a < x \leq b, \\ \dfrac{c-x}{c-b}, & b < x < c, \\ 0, & x \geq c, \end{cases} \tag{3.3}$$

Alternatif olarak, Gauss tipi üyelik fonksiyonu daha yumuşak geçiş sağlar ve aşağıdaki gibi ifade edilir (Denklem 3.4):

$$\mu(x) = \exp\left(-\frac{(x-c)^2}{2\sigma^2}\right) \tag{3.4}$$

Bulanık çıkarım sistemleri, genellikle şu biçimdeki kural setlerinden oluşur: R_i: "$Eğer\ x_1, A_1^i\ ise\ ve\ x_2, A_2^i\ ise, o\ zaman\ y, B^i\ olur$." Mamdani tipinde her kuralın sonucu bir bulanık kümedir.

Mamdani tipinde çıkarım sistemlerinde, her bir kuralın etkinlik derecesi minimum operatörü ile hesaplanır (Denklem 3.5):

$$\alpha_1 = \min\{\mu_{A_1^i}(x_1), \mu_{A_2^i}(x_2), \dots\} \tag{3.5}$$

Çıkarım sonucu birleşim operatörüyle elde edilir (Denklem 3.6):

$$\mu_{\tilde{B}}(y) = \max_i \left[\min\left(\alpha_i, \mu_{B^i}(y)\right)\right] \quad (3.6)$$

Çıktı kümesinin belirli bir değere indirgenmesi için sıklıkla ağırlıklı ortalama yöntemi (merkez yöntemi) kullanılır (Denklem 3.7):

$$y^* = \frac{\sum_{i=1}^{N} \alpha_i c_i}{\sum_{i=1}^{N} \alpha_i} \quad (3.7)$$

Burada y^*, durulaştırılmış çıktı değeri; α_i, i-inci kuralın etkinlik derecesi ve c_i: i-inci kuralın çıktı bulanık kümesinin merkez değeridir. Bu yapı sayesinde, bulanık mantık sistemleri çok kriterli, belirsiz ve doğrusal olmayan sistemlerin modellenmesine olanak tanır.

3.1.2. Uyarlamalı Nöro-Bulanık Çıkarım Sistemi (ANFIS)

ANFIS, bulanık mantık ile yapay sinir ağlarının birleşiminden oluşan hibrit bir sistemdir. Bu yapı, verilerden öğrenme kabiliyeti ile bulanık kuralları birleştirerek karmaşık ilişkileri modellemede yüksek doğruluk sağlar (Hoshino vd., 2024). Aşağıda ANFIS'in katmanlı mimarisi adım adım açıklanmıştır.

Bu katman, sistemin girdi değişkenlerini doğrudan bir sonraki katmana iletir. Giriş vektörü aşağıdaki şekilde ifade edilir (Denklem 3.8):

$$x = [x_1, x_2, \ldots, x_p] \quad (3.8)$$

Bu katmanda, her bir girdi değişkeni için birden fazla üyelik fonksiyonu (bulanık küme) tanımlıdır. Bu fonksiyonlar genellikle Gauss, üçgensel veya çan eğrisi şeklinde olabilir. Her bir üyelik fonksiyonunun çıktısı Denklem (3.9) ile gösterilir:

$$A_i^j = \mu_{A_i^j}(x_i) \tag{3.9}$$

Burada:

- x_i: i. giriş değişkeni
- A_i^j: x_i değişkenine ait j. Üyelik fonksiyonu
- $\mu_{A_i^j}(x_i)$: Üyelik derecesi

Bu katman, girişlerin tüm kombinasyonlarını içeren kuralların ateşleme seviyelerini hesaplar. Genellikle çarpım (AND) işlemi kullanılarak her bir kuralın ateşleme gücü w_k, Denklem (3.10) ile hesaplanır:

$$\bar{Q}_k = \prod_{i=1}^{p} \mu_{A_i^j}(x_i) = w_k \tag{3.10}$$

Burada M, toplam kural sayısı ve w_k ise k. kuralın ateşleme gücünü ifade eder.

Her kuralın ateşleme gücü, toplam ateşleme gücüne bölünerek normalize edilir. Normalleştirilmiş ateşleme gücü Denklem (3.11) ile verilir:

$$\widehat{w}_k = \frac{w_k}{\sum_{j=1}^{M} w_j} \tag{3.11}$$

Bu katman, her kuralın ağırlıklı çıktısını hesaplar ve tüm kural çıktılarının toplamını sistemin çıktısı olarak verir. Her bir kural için çıktılar, genellikle doğrusal fonksiyonlarla modellenir (Denklem 3.12):

$$f_k = \widehat{w}_k(m_k x_1 + n_k x_2 + \cdots + r_k x_p + s_k) \tag{3.12}$$

Son olarak, sistemin toplam çıktısı tüm kural katkılarıyla birlikte Denklem (3.13) ile hesaplanır:

$$F = \sum_{k=1}^{M} f_k = \sum_{k=1}^{M} \widehat{w}_k f_k \tag{3.13}$$

3.1.3. Genetik Algoritmalar

GA, Arama veya Çözüm uzayı S üzerinde çalışan, popülasyon tabanlı sezgisel optimizasyon yöntemleridir. Bu algoritmalar, evrimsel süreçleri modelleyerek çözüm kalitesini nesiller boyunca artırmayı hedefler (Mitchell, 1996). Aşağıda GA'nın temel bileşenlerinin matematiksel gösterimi ve ilişkili denklemler verilmiştir.

Başlangıç popülasyonu, S çözüm uzayından rastgele seçilen N adet bireyden oluşur (Denklem 3.14):

$$P^{(0)} = \left\{x_1^{(0)}, x_2^{(0)}, \dots, x_N^{(0)}\right\}, \qquad x_i^{(0)} \in S \tag{3.14}$$

Burada $P^{(0)}$, algoritmanın sıfırıncı nesildeki birey popülasyonunu; $x_i^{(0)}$ ise i. bireyin başlangıçtaki çözümünü temsil eder.

Her bireyin uygunluk seviyesi, problem özelinde tanımlanmış bir uygunluk fonksiyonu aracılığıyla hesaplanır:

$$f: S \to \mathbb{R}, \qquad f_i^{(t)} = f(x_i^{(t)}) \tag{3.15}$$

Denklem (3.15) ile gösterilen f fonksiyonu, bireyin mevcut çözüme olan katkısını kantitatif olarak ölçer; daha yüksek değerler, daha uygun bireyleri ifade eder. Uygunluk değerlerine bağlı olarak bireyler bir seçilim operatörü ile seçilir (Denklem 3.16):

$$S_{seçilim}^{(t)} = \mathcal{T}(P^{(t)}, f) \tag{3.16}$$

Burada $\mathcal{T}$, turnuva, rulet çarkı veya sıralı seçilim gibi yöntemlerle uygulanabilen seçim fonksiyonunu temsil eder. Bu işlem, güçlü bireylerin seçilme olasılığını artırarak elitizmi teşvik eder. Seçilen bireyler, çaprazlama işlemi ile yeniden kombinasyon sürecine tabi tutulur:

$$S_{çaprazlama}^{(t)} = \mathcal{C}\left(S_{seçilim}^{(t)}, \mathcal{p}_c\right) \tag{3.17}$$

Denklem (3.17)'teki $\mathcal{C}$ fonksiyonu, belirli bir çaprazlama olasılığı $\mathcal{p}_c \in [0,1]$ ile seçilen birey çiftlerinden yeni bireyler üretir. Bu aşama, çözüm uzayında keşif kabiliyetini artırır. Çaprazlamadan sonra oluşan bireyler, mutasyon operatörüyle küçük değişimlere uğratılır:

$$P^{(t+1)} = \mathcal{M}(S_{çaprazlama}^{(t)}, \mathcal{p}_m) \tag{3.18}$$

Burada $\mathcal{M}$, bireylerin genetik yapısına düşük olasılıkla ($\mathcal{p}_m \in [0,1]$) rastgele müdahalelerde bulunan mutasyon fonksiyonudur. Denklem (3.18), algoritmanın keşif-sömürü dengesini korumasına olanak tanır.

Algoritma, maksimum nesil sayısı T_{max} ya da belirli bir hedef uygunluk değerine f_{hedef} ulaşılana dek çalışır (Denklem 3.19):

$$Eğer\ t \geq T_{max}\ veya \max_{x \in P^t} f(x) \geq f_{hedef}, ise\ dur; aksi\ halde\ t \leftarrow t + 1 \tag{3.19}$$

Bu durdurma kriteri, algoritmanın ya belirlenen iterasyon sınırına ulaşması ya da yeterli çözüm kalitesine erişmesi durumunda çalışmasını sonlandırmasını sağlar.

3.1.4. Pekiştirmeli Öğrenme ve Derin Q Ağı (DQN)

Pekiştirmeli öğrenme, bir ajanin çevresiyle etkileşim yoluyla ödül maksimizasyonu için optimal politikayi öğrenmesini matematiksel olarak modelleyen bir yöntemdir. Bu süreç, genellikle bir Markov Karar Süreci (MDP) ile modellenir.

RL, bir MDP ile tanımlanır ve şu tuple ile ifade edilir (Zhao, 2025):

$$MDP = \langle S, A, R, P, \gamma \rangle \tag{3.20}$$

Burada:

- S: Durum uzayı, ajanın bulunabileceği tüm durumların kümesi (sonlu veya sürekli).
- A: Eylem uzayı, ajanın gerçekleştirebileceği tüm eylemlerin kümesi (sonlu veya sürekli)
- $P(s'|s,a)$: Durum geçiş olasılığı, $s \in S$ durumunda $a \in A$ eylemi sonrası $s' \in S$ durumuna geçme olasılığı.
- $R(s,a,s')$: Ödül fonksiyonu, s-den s'-ye a eylemiyle geçiş için alınan ödül.
- $\gamma \in [0,1)$: İndirim faktörü, gelecekteki ödüllerin bugünkü değerini ayarlar.

Ajan, bir politika $\pi(a|s)$ ile hareket eder. Amaç beklenen kümülatif ödülü maksimize eden politikayı bulmaktır:

$$J(\pi) = \mathbb{E}_\pi \left[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t, s_{t+1}) \right] \tag{3.21}$$

Burada:

- $J(\pi)$: Politika π'nin beklenen kümülatif ödülü.
- $\mathbb{E}_\pi$: Politika π'ye göre beklenen değer.
- s_t, a_t, s_{t+1}: Zaman adımı t'deki durum, eylem ve sonraki durum.

- $\mu(s)$: Başlangıç durum dağılımı, $s_0 \sim \mu(s)$.
- γ^t: İndirim faktörü, t adım sonrasındaki ödülün ağırlığını belirler.

Denklem (3.21), Pekiştirmeli öğrenmenin temel optimizasyon hedefini tanimlar.

Değer Fonksiyonları, politikaların kalitesini ölçer. Durum-değer fonksiyonu şu şekildedir:

$$V^{\pi}(s) = \mathbb{E}_{\pi}\left[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t, s_{t+1}) \mid s_0 = s\right] \tag{3.22}$$

Burada:

- $V^{\pi}(s)$: s durumunda politika π'yi izleyerek elde edilen beklenen kümülatif ödül.
- $s_0 = s$: Başlangıç durumunun s olduğu koşulu.

Eylem-değer fonksiyonu ise:

$$Q^{\pi}(s, a) = \mathbb{E}_{\pi}\left[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t, s_{t+1}) \mid s_0 = s, \quad a_0 = a\right] \tag{3.23}$$

Burada:

- $Q^{\pi}(s, a)$: s durumunda a eylemini seçip sonra politika π'yi izleyerek elde edilen beklenen kümülatif ödül.
- $a_0 = a$: İlk eylemin a olduğu koşulu.

Bu fonksiyonlar arasında şu ilişkiler vardır:

$$V^{\pi}(s) = \sum_{a \in A} \pi(a|s) Q^{\pi}(s, a) \tag{3.24}$$

$$Q^{\pi}(s, a) = \mathbb{E}_{s' \sim P(\cdot|s, a)}[R(s, a, s') + \gamma V^{\pi}(s')] \tag{3.25}$$

Burada:

- $\pi(a|s)$: s durumunda a eylemini seçme olasılığı.
- $\mathbb{E}_{s' \sim P(\cdot|s,a)}$: s''nin $P(\cdot\,|s,a)$'ya göre beklenen değeri.

Denklem (3.24) ve (3.25), değer fonksiyonlarının politika ve çevre dinamikleriyle ilişkişini gösterir.

Değer fonksiyonları, Bellman denklemleriyle ifade edilir (Lapan, 2024). Durum-değer için:

$$V^{\pi}(s) = \sum_{a \in A} \pi(a|s) \sum_{s' \in S} P(s'|s,a)[R(s,a,s') + \gamma V^{\pi}(s')] \tag{3.26}$$

Burada:

- $\sum_{a \in A}$: Tüm eylemler üzerinde toplama.
- $\sum_{s' \in S}$: Tüm sonraki durumlar üzerinde toplama.

Eylem-değer için:

$$Q^{\pi}(s,a) = \sum_{s' \in S} P(s'|s,a) \left[R(s,a,s') + \gamma \sum_{a' \in A} \pi(a'|s') Q^{\pi}(s',a') \right] \tag{3.27}$$

Burada:

- $\sum_{a' \in A}$: Sonraki durumda seçilebilecek tüm eylemler üzerinde toplama.

Optimal politika için Bellman optimalite denklemleri:

$$V^{*}(s) = \max_{a \in A} \sum_{s' \in S} P(s'|s,a)[R(s,a,s') + \gamma V^{\pi}(s')] \tag{3.28}$$

$$Q^*(s,a) = \sum_{s' \in S} P(s'|s,a) \left[R(s,a,s') + \gamma \max_{a' \in A} Q^*(s',a') \right] \quad (3.29)$$

Burada:

- $max_{a \in A}$: En yüksek değeri veren eylemi seçme.
- $V^*(s)$, $Q^*(s,a)$: Optimal politika altındaki değer fonksiyonları.

Denklem (3.28) ve (3.29), optimal politikayı tanımlayan temel denklemlerdir.

Optimal politikayı bulmak için iki ana yöntem kullanılır:

Değer İterasyonu:

$$V_{k+1}(s) = \max_{a \in A} \sum_{s' \in S} P(s'|s,a)[R(s,a,s') + \gamma V_k(s')] \quad (3.30)$$

Burada:

- $V_{k+1}(s)$, V_k: $k+1$ ve k'inci iterasyondaki durum-değer fonksiyonları.

Denklem (3.30), $V_k \rightarrow V^*$ için iterasyon yapar.

Politika İterasyonu:

Politika değerlendirme:

$$V(s) = \sum_{a \in A} \pi(a|s) \sum_{s' \in S} P(s'|s,a)[R(s,a,s') + \gamma V(s')] \quad (3.31)$$

Politika iyileştirme:

$$\pi'(s) = \arg\max_{a \in A} \sum_{s' \in S} P(s'|s,a)[R(s,a,s') + \gamma V^{\pi}(s')] \quad (3.32)$$

Burada:

- $\pi'(s)$: İyileştirilmiş politika.
- $\arg max$: Maksimum Değeri sağlayan eylemi seçme.

Model-free bir algoritma olan Q-Öğrenme:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left[R(s_t, a_t, s_{t+1}) + \gamma \max_{a' \in A} Q(s_{t+1}, a') - Q(s_t, a_t) \right] \tag{3.33}$$

Burada:

- α: Öğrenme oranı, güncelleme adım büyüklüğünü kontrol eder.
- $R(s_t, a_t, s_{t+1})$: t'inci adımda alınan ödül.
- $max_{a' \in A} Q(s_{t+1}, a')$: Sonraki durumdaki en iyi eylemin değeri.

Denklem (3.33), model bilgisi olmadan Q-fonksiyonunu günceller.

Politika $\pi_\theta(a|s)$ parametrelendirir ve gradyan:

$$\nabla_\theta J(\pi_\theta) = \mathbb{E}_{\pi_\theta} \left[\sum_{t=0}^{\infty} \nabla_\theta \log \pi_\theta(a_t|s_t) Q^{\pi_\theta}(s_t, a_t) \right] \tag{3.34}$$

Burada:

- θ: Politikanın parametreleri.
- ∇_θ: Parametrelere göre gradyan.
- $\log \pi_\theta(a_t|s_t)$: Politikanın logaritmik olasılığı

REINFORCE algoritması:

$$\nabla_\theta J(\pi_\theta) \approx \sum_{t=0}^{T} \nabla_\theta \log \pi_\theta(a_t|s_t) \left(\sum_{k=t}^{T} \gamma^{k-t} R(s_t, a_t, s_{t+1}) \right) \tag{3.35}$$

Burada:

- T: Bir bölümün uzunluğu
- $\sum_{k=t}^{T} \gamma^{k-t} R$: t'den itibaren indirimli ödül toplamı.

Denklem (3.35), politika optimizasyonunun temelini oluşturur.

Aktör (π_θ) ve eleştirmen (Q_w) için:

$$\nabla_\theta J(\pi_\theta) = \mathbb{E}_{\pi_\theta}[\nabla_\theta \log \pi_\theta(a|s) Q_w(s,a)] \tag{3.36}$$

Avantaj fonksiyonu:

$$A^\pi(s,a) = Q^\pi(s,a) - V^\pi(s) \tag{3.37}$$

Burada:

- $Q_w(s,a)$: Eleştirmenin tahmin ettiği eylem-durum fonksiyonu.
- $A^\pi(s,a)$: Avantaj fonksiyonu, eylemin relatif değerini ölçer.

Deterministik Politika Gradyanı (DPG):

$$\nabla_\theta J(\mu_\theta) = \mathbb{E}\left[\nabla_\theta \mu_\theta(s) \nabla_a Q(s,a)|_{a=\mu_\theta(s)}\right] \tag{3.38}$$

Burada:

- $\mu_\theta(s)$: Deterministik politika.
- $\nabla_a Q(s,a)$: Q-fonksiyonunun eyleme göre türevi.

Denklem (3.38), sürekli eylem uzaylarında kullanılır.

Yumuşak Oyuncu-Eleştirmen Algoritması (SAC):

$$J(\pi) = \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^t \left(R(s_t, a_t, s_{t+1}) + \alpha \mathcal{H}\left(\pi(\cdot|s_t)\right)\right)\right] \tag{3.39}$$

Burada:

- $\mathcal{H}(\pi) = -\sum_a \pi(a|s) \log \pi(a|s)$: Politikanın entropisi.
- α: Entropi katsayısı, keşif ve istismar dengesini ayarlar.

Derin Q Ağı (DQN), Q-öğrenmeyi derin sinir ağlarıyla birleştirerek yüksek boyutlu durum uzaylarında etkili bir şekilde çalışır. Q-fonksiyonu, parametreleri θ olan

bir sinir ağı $Q(s, a; \theta)$ ile temsil edilir. DQN, iki temel teknik kullanır: Deneyim tekrarı ve hedef ağ.

DQN'nin güncelleme kuralı şu şekildedir:

$$Q(s_t, a_t; \theta) \leftarrow Q(s_t, a_t; \theta) + \alpha \left[r_t + \gamma \max_{a' \in A} Q(s_{t+1}, a'; \theta^-) - Q(s_t, a_t; \theta) \right] \tag{3.40}$$

Burada:

- $Q(s_t, a_t; \theta)$: Hedef Q-ağı, θ parametreleriyle.
- $Q(s_t, a_t; \theta^-)$: Hedef Q-ağı, sabit parametreler θ^- ile.
- r_t: t'inci adımda alınan ödül, $r_t = R(s_t, a_t, s_{t+1})$.
- α: Öğrenme oranı.
- γ: İndirim faktörü.

Hedef ağ parametreleri θ^-, periyodik olarak güncel ağdan kopyalanır veya yavaşça güncellenir:

$$\theta^- \leftarrow \tau\theta + (1 - \tau)\theta^- \tag{3.41}$$

Burada:

- τ: Hedef ağ güncelleme oranı, genellikle küçük bir sabit (örneğin, $\tau = 0.005$).

Deneyim tekrarı için, geçişler (s_t, a_t, s_{t+1}) bir tamponda saklanır ve rastgele örneklenerek güncellemelerde kullanılır. Kayıp fonksiyonu şu şekildedir:

$$L(\theta) = \mathbb{E}_{(s,a,r,s') \sim \mathcal{D}} \left[\left(r + \gamma \max_{a' \in A} Q(s', a'; \theta^-) - Q(s, a; \theta) \right)^2 \right] \tag{3.42}$$

Burada:

- $\mathcal{D}$: Deneyim tekrarı tamponu.
- $L(\theta)$: Karesel hata kaybı, Q-değerlerini hedefe yaklaştırmak için minimize edilir.

DQN, ϵ-greedy politika ile keşfi destekler:

$$\pi(s) = \begin{cases} \arg max_{a \in A} Q(s, a; \theta), & olasılık\ 1 - \epsilon \\ rastgele\ a \in A, & olasılık\ \epsilon \end{cases} \tag{3.43}$$

Burada:

- ϵ: Keşif oranı, genellikle zamanla azaltılır.

Pekiştirmeli öğrenme, Markov Karar Süreci çerçevesinde (Denklem (3.20)), ajanın çevre ile etkileşimi yoluyla ödül maksimizasyonu sağlayan optimal politikayı öğrenmesini sağlar. Durum ve eylem-değer fonksiyonları (Denklem (3.22), (3.23)) ile Bellman denklemleri (Denklem (3.26), (3.28)), Pekiştirmeli öğrenmenin teorik temelini oluşturur. Q-öğrenme (Denklem (3.33)), politika gradyanı (Denklem (3.34)), aktör-eleştirmen (Denklem (3.36)) ve DQN (Denklem (3.40), (3.42)) gibi optimizasyon yöntemleri, bu temeli pratik algoritmalara (REINFORCE, DPG, SAC, DQN) dönüştürür. DQN, yüksek boyutlu durum uzaylarında derin sinir ağlarıyla Q-öğrenmeyi etkili bir şekilde genişletir.

3.1.5. Karar Ağaçları

Problem Tanımı: Veri kümesi $\mathcal{D} = \{(x^{(i)}, y^{(i)})\}_{i=1}^{N}$ burada $x^{(i)} \in \mathbb{R}^d$, $y^{(i)} \in \mathcal{Y} \subseteq \mathbb{R}$, ve d özellik sayısını ifade eder. Karar ağacı, $\mathcal{D}$ kümesini özellik uzayında bölerek bir hiyerarşik yapı oluşturur.

Düğüm Bölme Yapısı: Bir düğüm v altında bulunan örnek alt kümesi $S_v \subseteq \mathcal{D}$ olarak tanımlanır. Her bölme, bir özellik-indeks ve eşik çifti $\varphi = (f, \tau)$ ile ifade edilir. Bu bölme sonucunda veri iki alt kümeye ayrılır:

Sol:

$$S_v^L(\varphi) = \{(x, y) \in S_v \mid x_f \leq \tau\} \tag{3.44}$$

Sağ:

$$S_v^R(\varphi) = S_v \backslash S_v^R(\varphi) \tag{3.45}$$

Bölme Maliyeti: Verilen bir safsızlık ölçütü $\Psi(\cdot)$ kullanılarak, bölmenin maliyeti şu şekilde ifade edilir:

$$C(S_v, \varphi) = \frac{|S_v^L|}{|S_v|}\Psi(S_v^L) + \frac{|S_v^R|}{|S_v|}\Psi(S_v^R) \tag{3.46}$$

Optimal bölme, şu şekilde seçilir:

$$\varphi^* = \arg\min_{\varphi \in \Phi} C(S_v, \varphi) \tag{3.47}$$

Sınıflandırma Safsızlık Ölçütleri: Her düğümdeki sınıf dağılımı için:

$$p_k^{(v)} = \frac{1}{|S_v|} \sum_{(x,y)\in S_v} 1[y = k] \tag{3.48}$$

Gini İndeksi:

$$\Psi(S_v) = \sum_k p_k^{(v)}(1 - p_k^{(v)}) \tag{3.49}$$

Entropi:

$$\Psi(S_v) = -\sum_k p_k^{(v)} \log p_k^{(v)} \tag{3.50}$$

Çapraz Entropi (Log Loss):

Eğer tahmin edilen olasılıklar $\hat{p}_k(x)$ ise:

$$\mathrm{LL}(\mathcal{D}) = \frac{1}{|\mathcal{D}|} \sum_{(x,y)\in\mathcal{D}} \log \hat{p}_y(x) \tag{3.51}$$

Regresyon Safsızlık Ölçütleri: Her düğümde hedef değerlerin ortalaması:

$$\bar{y}_v = \frac{1}{|S_v|} \sum_{(x,y)\in S_v} y \tag{3.52}$$

Ortalama Kare Hata (MSE):

$$\Psi(S_v) = \frac{1}{|S_v|} \sum_{(x,y)\in S_v} (y - \bar{y}_v)^2 \tag{3.53}$$

Poisson Sapması (pozitif hedefler için):

$$\Psi(S_v) = \frac{2}{|S_v|} \sum_{(x,y)\in S_v} (y \log \frac{y}{\bar{y}_v} - y + \bar{y}_v)^2 \tag{3.54}$$

Ortalama Mutlak Hata (MAE):

$$\Psi(S_v) = \frac{1}{|S_v|} \sum_{(x,y)\in S_v} |y - \tilde{y}_v| \tag{3.55}$$

burada $\tilde{y}_v$ medyandır:

$$\tilde{y}_v = median(\{y \mid (x,y) \in S_v\}) \tag{3.56}$$

3.1.6. Doğrusal Diskriminant Analizi (LDA)

LDA, sınıflar arasındaki ayrımı artırmak ve boyutu azaltmak için verinin doğrusal dönüşümünü sağlayan bir yöntemdir. Bu yöntem, sınıf içi dağılımı minimize ederken sınıflar arası dağılımı maksimize etmeyi amaçlar.

LDA, N adet D-boyutlu özellik vektörü $x_1, x_2, \dots, x_N \in \mathbb{R}^D$ ve bunlara karşılık gelen sınıf etiketleri $y_1, y_2, \dots, y_N \in \{1,2, \dots, C\}$ içeren bir veri seti üzerinde çalışır. Amaç, $\mathcal{W} \in \mathbb{R}^{D \times k}$ dönüşüm matrisini bulmaktır; burada $k \leq C - 1$, sınıflar arası dağılımı maksimize ederken sınıf içi dağılımı minimize eder.

Veri seti tanımları:

$$u = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{3.57}$$

$$u_k = \frac{1}{N_k} \sum_{i:y_i=k} x_i \tag{3.58}$$

Burada:

- u: Tüm veri setinin ortalama vektörü.
- u_k: k-inci sınıfın ortalama vektörü.
- N: Toplam örnek sayısı.
- N_k: k-inci sınıftaki örnek sayısı.
- C: Toplam sınıf sayısı.

Sınıf içi dağılım matrisi S_w, her sınıfın içindeki örneklerin dağılımını ölçer:

$$S_w = \sum_{k=1}^{C} \sum_{i:y_i=k} (x_i - u_k)(x_i - u_k)^T \tag{3.59}$$

Burada:

- $S_w \in \mathbb{R}^{D \times D}$: Sınıf içi dağılım matrisi.
- $x_i - u_k$: k-inci sınıftaki i-inci örneğin, sınıf ortalamasından farkı.
- $(\cdot)^T$: Vektörün transpozu.

Sınıflar arası dağılım matrisi, S_b, sınıf ortalamalarının genel ortalamaya göre dağılımını ölçer:

$$S_b = \sum_{k=1}^{C} N_k (u_k - u)(u_k - u)^T \tag{3.60}$$

Burada:

- $S_b \in \mathbb{R}^{D \times D}$: Sınıflar arası dağılım matrisi.
- $u_k - u$: k-inci sınıf ortalamasının genel ortalamadan farkı.
- N_k: k-inci sınıftaki örnek sayısı.

LDA, sınıflar arası dağılımı maksimize ederken sınıf içi dağılımı minimize eden bir dönüşüm matrisi $\mathcal{W}$ bulmayı hedefler. Bu, genelleştirilmiş özdeğer problemi olarak ifade edilir:

$$S_w^{-1} S_b w = \lambda w \tag{3.61}$$

Burada:

- S_w^{-1}: Sınıf içi dağılım matrisinin tersi.
- w: Özvektör, projeksiyon yönünü temsil eder.
- λ: Özdeğer, sınıflar arası ayrımın ölçüsü.

En büyük $k - 1$ özdeğere karşılık gelen özvektörler, $\mathcal{W}$ matrisinin sütunlarını oluşturur. Denklem (3.61), LDA'nın temel optimizasyon problemini tanımlar.

LDA, orijinal özellik vektörlerini daha düşük boyutlu bir uzaya projekte eder:

$$z = \mathcal{W}^T x \tag{3.62}$$

Burada:

- $z \in \mathbb{R}^k$: Projekte edilmiş k boyutlu vektör.
- $\mathcal{W}^T$: Dönüşüm matrisinin transpozu.
- $x \in \mathbb{R}^D$: Orijinal D boyutlu özellik vektörü.

Denklem (3.62), LDA'nın boyut azaltma işlemini gösterir.

Yeni bir veri noktası x için sınıflandırma, LDA alt uzayında en yakın sınıf ortalamasına göre yapılır:

$$\hat{y} = \arg\min_k \|\mathcal{W}^T x - \mathcal{W}^T u_k\|_2 \tag{3.63}$$

Burada:

- $\hat{y}$: Tahmin edilen sınıf etiketi.
- $\|\cdot\|_2$: Öklid mesafesi.
- $\mathcal{W}^T u_k$: k-inci sınıfın projekte edilmiş ortalaması.

Denklem (3.63), LDA'nın sınıflandırma sürecini tanımlar.

LDA, Fisher kriterini maksimize eder (Ishwaran, 2025):

$$J(\mathcal{W}) = \frac{|\mathcal{W}^T S_b \mathcal{W}|}{|\mathcal{W}^T S_w \mathcal{W}|} \tag{3.64}$$

Burada:

- $J(\mathcal{W})$: Fisher kriteri, sınıflar arası ve sınıflar içi dağılımların oranını ölçer.
- $|\cdot|$: Matrisin determinantı.

LDA, sınıflar arası dağılımı maksimize ederken sınıf içi dağılımı minimize eden bir dönüşüm matrisi bulur (Denklem (3.61)). Sınıf içi ve sınıflar arası dağılım matrisleri (Denklem (3.59), (3.60)) ile tanımlanan bu süreç, boyut azaltma (Denklem (3.62)) ve sınıflandırma (Denklem (3.63)) için kullanılır. Fisher kriteri (Denklem (3.64)), LDA'nın optimizasyon hedefini özetler ve yöntemin teorik temelini sağlar.

3.1.7. Lojistik Regresyon

Lojistik regresyon ikili veya çok sınıflı sınıflandırma problemlerinde kullanılan bir istatistiksel ve makine öğrenmesi yöntemidir. Bir veri noktasının belirli bir sınıfa ait olma olasılığını modellemek için lojistik (sigmoid) fonksiyonunu kullanır ve parametreleri maksimum olabilirlik tahmini ile optimize eder (Jurafsky & Martin, 2025).

Lojistik regresyon, N adet D-boyutlu özellik vektörü $x_1, x_2, \dots, x_N \in \mathbb{R}^D$ ve bunlara karşılık gelen sınıf etiketleri $y_1, y_2, \dots, y_N \in \{0,1\}$ içeren bir veri seti üzerinde çalışır. Amaç, x_i özellik vektörüne göre $y_i = 1$ olma olasılığını tahmin etmektir.

Lojistik regresyon, bir veri noktasının sınıf-1'e ait olma olasılığını şu şekilde modeller:

$$P(y_i = 1|x_i, w, b) = \sigma(w^T x_i + b) \tag{3.65}$$

Burada:

- $P(y_i = 1|x_i, w, b)$: x_i için sınıf-1'e ait olma olasılığı.
- $\sigma(z) = \frac{1}{1+e^{-z}}$: Sigmoid fonksiyonu.
- $w \in \mathbb{R}^D$: Ağırlık vektörü.
- $b \in \mathbb{R}^D$: Sapma (bias) terimi.
- $w^T x_i$: Özellik vektörü ile ağırlıkların iç çarpımı.

Sigmoid fonksiyonu şu şekilde tanımlanır:

$$\sigma(z) = \frac{1}{1 + \exp(-z)} \tag{3.66}$$

Burada:

- z: Girdi değeri, genellikle $w^T x_i + b$.
- exp (·): Üstel fonksiyon.

Denklem (3.65), lojistik regresyonun olasılık modelini tanımlar.

Sınıf-0 için olasılık:

$$P(y_i = 0|x_i, w, b) = 1 - \sigma(w^T x_i + b) \tag{3.67}$$

Genel olarak, olasılık dağılımı tek bir ifade ile yazılabilir:

$$P(y_i|x_i, w, b) = [\sigma(w^T x_i + b)]^{y_i}[1 - \sigma(w^T x_i + b)]^{1-y_i} \tag{3.68}$$

Lojistik regresyon, parametreleri (w, b) maksimum olabilirlik tahmini (Maximum Likelihood Estimation, MLE) ile optimize eder. Olabilirlik fonksiyonu:

$$L(w, b) = \prod_{i=1}^{N} P(y_i|x_i, w, b) \tag{3.69}$$

Log-Olabilirlik fonksiyonu, optimizasyonu kolaylaştırmak için kullanılır:

$$\ell(w, b) = \sum_{i=1}^{N} \left[y_i \log \sigma(w^T x_i + b) + (1 - y_i) \log\left(1 - \sigma(w^T x_i + b)\right)\right] \tag{3.70}$$

Burada:

- $\ell(w, b)$: Log-Olabilirlik fonksiyonu.
- N: Veri noktası sayısı.

Denklem (3.70), modelin optimizasyon hedefini tanımlar.

Lojistik regresyonun kayıp fonksiyonu, negatif Log-Olabilirlik (cross-entropy kaybı) olarak ifade edilir:

$$J(w,b) = -\sum_{i=1}^{N}\left[y_i \log \sigma(w^T x_i + b) + (1-y_i)\log\left(1-\sigma(w^T x_i + b)\right)\right] \tag{3.71}$$

Burada:

- $J(w,b)$: Minimize edilmesi gereken kayıp fonksiyonu.

Denklem (3.71), lojistik regresyonun parametre optimizasyonunu yönlendirir.

Kayıp Fonksiyonunu minimize etmek için gradyan inişi kullanılır. $J(w,b)$'nin w ve b'ye göre kısmi türevleri:

$$\frac{\partial J}{\partial w} = \sum_{i=1}^{N}(\sigma(w^T x_i + b) - y_i)x_i \tag{3.72}$$

$$\frac{\partial J}{\partial b} = \sum_{i=1}^{N}(\sigma(w^T x_i + b) - y_i) \tag{3.73}$$

Burada:

- $\frac{\partial J}{\partial w}$: Ağırlıklara göre gradyan.
- $\frac{\partial J}{\partial b}$: Sapma terimine göre gradyan.
- $\sigma(w^T x_i + b) - y_i$: Tahmin hatası.

Gradyan inişi güncellemeleri:

$$w \leftarrow w - \alpha\frac{\partial J}{\partial w}, \qquad b \leftarrow b - \alpha\frac{\partial J}{\partial b} \tag{3.74}$$

Burada:

- α: Öğrenme oranı, güncelleme adım büyüklüğünü kontrol eder.

Denklem (3.74), parametrelerin iteratif olarak güncellenmesini sağlar.

Yeni bir veri noktası x için sınıf tahmini şu şekilde yapılır:

$$\hat{y} = \begin{cases} 1, & eğer\ \sigma(w^T x_i + b) \geq 0.5 \\ 0, & eğer\ \sigma(w^T x_i + b) < 0.5 \end{cases} \tag{3.75}$$

Denklem (3.75), lojistik regresyonun sınıflandırma kararını tanımlar.

3.1.8. K-En Yakın Komşu (KNN)

KNN, denetimli öğrenmede kullanılan bir sınıflandırma ve regresyon algoritmasıdır. Yeni bir veri noktasını, eğitim veri setindeki en yakın K adet komşusunun sınıf etiketlerine göre sınıflandırır veya değer tahmin eder. KNN, model eğitimi gerektirmez ve mesafe tabanlı bir yaklaşım kullanır. KNN, N adet D-boyutlu özellik vektörü $x_1, x_2, \dots, x_N \in \mathbb{R}^D$ ve bunlara karşılık gelen sınıf etiketleri $y_1, y_2, \dots, y_N \in \{0,1, \dots, C-1\}$ içeren bir eğitim veri seti $\tau = \{(x_i, y_i)\}_{i=1}^N$ üzerinde çalışır. Amaç, yeni bir veri noktası $x \in \mathbb{R}^D$ için sınıf etiketi $\hat{y}$ tahmin etmektir (Kroese vd., 2020)

KNN, veri noktalarının yakınlığını ölçmek için bir mesafe metriği kullanır. Yaygın olarak Oklid mesafesi tercih edilir:

$$d(x, x_i) = \sqrt{\sum_{j=1}^{D} \left(x_j - x_{i,j}\right)^2} \tag{3.76}$$

Burada:

- $d(x, x_i)$: x ve x_i arasındaki Oklid mesafesi.
- x_j, $x_{i,j}$: x ve x_i'nin j-inci boyutlardaki değerleri.
- D: Özellik uzayının boyutu.

Denklem (3.76), KNN'nin mesafe hesaplamasını tanımlar.

Yeni veri noktası x için, eğitim veri setindeki tüm noktalarla mesafeler hesaplanır ve mesafeye göre sıralanır: $x_{(1)}, x_{(2)}, \dots, x_{(N)}$, burada $d\left(x, x_{(1)}\right) \leq d\left(x, x_{(2)}\right) \leq \cdots \leq d\left(x, x_{(N)}\right)$.

En yakın K noktanın alt kümesi:

$$\tau_K(x) = \left\{\left(x_{(i)}, y_{(i)}\right)\right\}_{i=1}^{K} \tag{3.77}$$

Burada:

- $\tau_K(x)$: x'e en yakın K adet veri noktasını ve etiketlerini içeren küme.
- $x_{(i)}, y_{(i)}$: i-inci en yakın noktanın özellik vektörü ve sınıf etiketi.
- K: Komşu sayısı, kullanıcı tarafından belirlenen bir hiperparametre.

Denklem (3.77), sınıflandırma için komşu kümesini tanımlar.

KNN, $\tau_K(x)$ içindeki sınıf etiketlerinin en sık görülenine göre sınıflandırma yapar. Sınıf oyları, her sınıf için komşu etiketlerinin sayısı olarak hesaplanır:

$$V_c = \sum_{(x_{(i)}, y_{(i)}) \in \tau_K(x)} \mathbf{1}\{y_{(i)} = c\} \tag{3.78}$$

Sınıf tahmini:

$$\hat{y} = \arg \max_{c \in \{0,1,\dots,C-1\}} V_c \tag{3.79}$$

Burada:

- V_c: Sınıf c'nin aldığı oy sayısı.
- $\mathbf{1}\{y_{(i)} = c\}$: $y_{(i)} = c$ ise 1, değilse 0 olan gösterge fonksiyonu.
- $\hat{y}$: x için tahmin edilen sınıf etiketi.

- $\arg max$: En yüksek oyu alan sınıfı seçme.

Eğer birden fazla sınıf aynı oyu alırsa, eşit olasılıkla rastgele bir seçim yapılır. Denklem (3.79), KNN'nin sınıflandırma kuralını tanımlar.

$K = 1$ durumunda, sadece en yakın komşu dikkate alınır:

$$\hat{y} = y_{(1)} \tag{3.80}$$

Burada:

- $y_{(1)}$: x'e en yakın noktanın sınıf etiketi.

Denklem (3.80), 1-NN kuralını tanımlar.

$K = 1$ için, özellik uzayı $\mathbb{R}^D$, her veri noktası x_i için bir Voronoi bölgesine bölünür:

$$R_i = \{x \in \mathbb{R}^D : d(x, x_i) \leq d(x, x_j), \forall j \neq i\} \tag{3.81}$$

Burada:

- R_i: x_i'ye en yakın tüm noktaların oluşturduğu Voronoi bölgesi.

Denklem (3.81), 1-NN için uzay bölünmesini tanımlar.

Ağırlıklı KNN, komşuların mesafelerine bağlı olarak oyları ağırlıklandırır. Gaussian kernel bazlı bir ağırlık fonksiyonu kullanılabilir:

$$w_i = \exp\left(-\frac{d(x, x_i)^2}{2\sigma^2}\right) \tag{3.82}$$

Ağırlıklı sınıflandırma kuralı:

$$\hat{y} = \arg \max_{c \in \{0,1,\ldots,C-1\}} \sum_{(x_{(i)}, y_{(i)}) \in \tau_K(x)} w_i \mathbf{1}\{y_{(i)} = c\} \tag{3.83}$$

Burada:

- w_i: i-inci komşu için ağırlık, mesafeye bağlı olarak hesaplanır.
- σ: Gaussian kernelin bant genişliği parametresi.

Denklem (3.83), mesafeye duyarlı sınıflandırmayı tanımlar.

3.2. Veri Setlerinin İncelenmesi ve Hazırlanması

Bu alt bölümde, çalışmada kullanılan üç farklı siber güvenlik veri seti—CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset—ayrı ayrı ele alınarak içerik özellikleri, saldırı türleri ve veri boyutları bakımından değerlendirilmiştir. Her bir veri seti, model performansını test etmek için belirli ön işleme ve etiketleme adımlarına tabi tutulmuş; bu işlemler ayrıntılı olarak sunulmuştur.

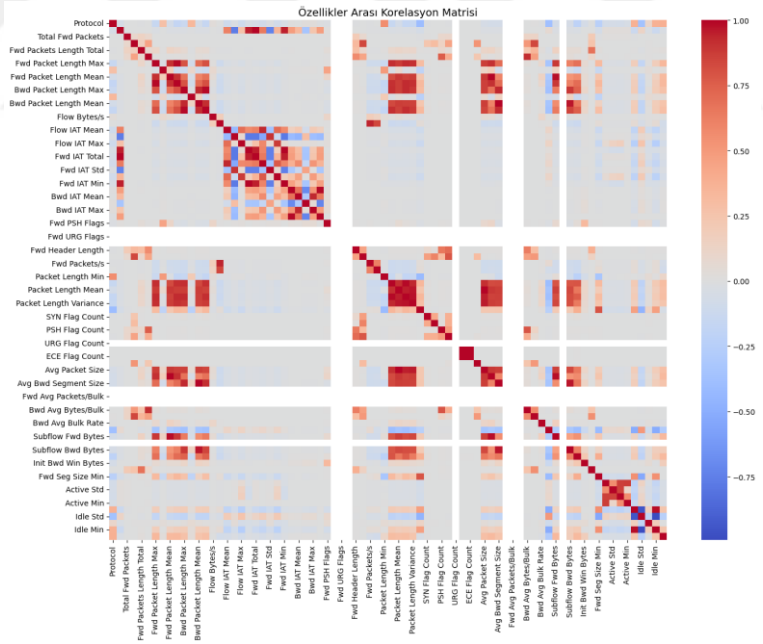
Bu çalışmada kullanılan Edge-IIoTset, CSE-CIC-IDS2018 ve CIC-ToN-IoT veri setleri, model eğitimi öncesinde kapsamlı bir ön işleme sürecine tabi tutulmuştur. İlk olarak, verilerdeki gürültü ve anlamsız bilgiler ayıklanmış; aykırı değerler Z-skoru ve IQR yöntemleriyle tespit edilerek uygun şekilde düzeltilmiş ya da veri kümesinden çıkarılmıştır. Eksik veriler, durumun niteliğine bağlı olarak silme veya istatistiksel tahmin yöntemleriyle tamamlanmıştır. Anomali tespiti sürecinde, yalnızca geleneksel yöntemlerle sınırlı kalınmamış; bunun yerine yapay sinir ağları ve makine öğrenmesi algoritmalarının yanı sıra bulanık mantık ve genetik algoritma gibi yumuşak hesaplama yaklaşımlarından ve bu yöntemlerin birleşiminden oluşan hibrit modellerden yararlanılmıştır. Bu adımlar sayesinde, modele sunulacak verinin güvenilirliği ve bütünlüğü artırılarak öğrenme sürecinde oluşabilecek hataların önüne geçilmiştir.

Devamında, tüm değişkenlerin öğrenme sürecine eşit katkı sunabilmesi amacıyla Min-Max ve Z-skoru gibi standartlaştırma teknikleri uygulanmış; veri dağılımını iyileştirmek için Box-Cox dönüşümü gerçekleştirilmiştir. Özellikle sınıf dengesizliği bulunan durumlarda, azınlık sınıfların temsiliyetini artırmak amacıyla Sentetik Azınlık Aşırı Örnekleme Tekniği (SMOTE) kullanılarak sentetik örnekler üretilmiş ve eğitim

verisine entegre edilmiştir. Bu sayede sınıflar arası denge sağlanmış ve modelin azınlık sınıfları doğru şekilde öğrenme kapasitesi artırılmıştır.

Elde edilen temiz ve normalize edilmiş veri setleri, genellikle %80 eğitim, %10 doğrulama ve %10 test oranlarında olacak şekilde bölünmüş; veri türüne göre zamana dayalı ya da sınıf dengesini koruyacak biçimde tabakalı örnekleme teknikleri tercih edilmiştir. Modelin genellenebilirliğini sağlamak ve aşırı öğrenmeyi önlemek adına k-katlı çapraz doğrulama, tabakalı çapraz doğrulama ve zaman serisi doğrulama gibi stratejiler kullanılmıştır. Özellik seçimi aşamasında, korelasyon analizi, karşılıklı bilgi kazancı ve model tabanlı önem sıralama yöntemleri aracılığıyla anlamlı öznitelikler belirlenmiş ve böylece modelin hem doğruluk seviyesi hem de işlem verimliliği optimize edilmiştir. Son olarak, boyut indirgeme teknikleri (PCA, LDA, t-SNE) uygulanarak veri uzayı sadeleştirilmiş; bu sayede hem bilgi kaybı en aza indirilmiş hem de hesaplama maliyetleri düşürülerek modelin genel performansı artırılmıştır.

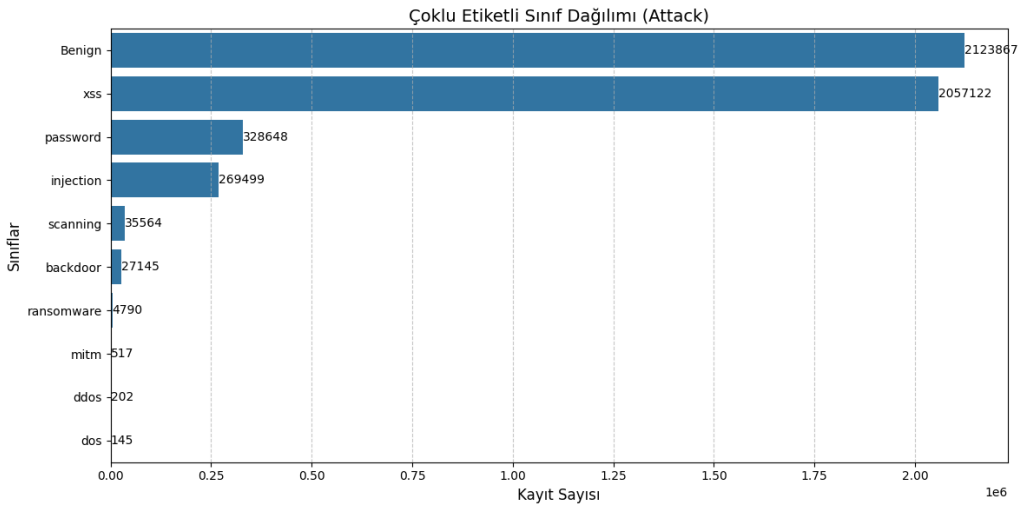
3.2.1. CIC-ToN-IoT Veri Seti



Şekil 3.1. CIC-ToN-IoT veri setinde özellikler arası korelasyon matrisi

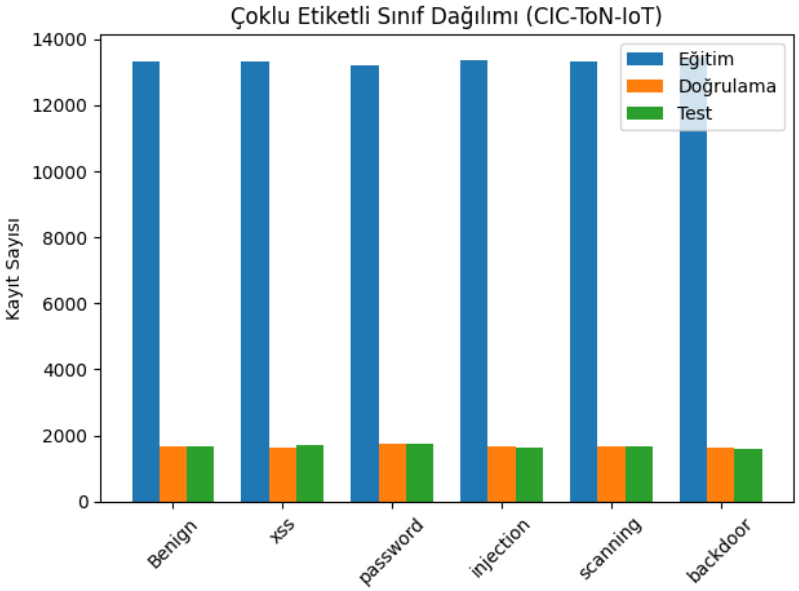
Şekil 3.1, CIC-ToN-IoT veri setindeki özellikler (örneğin, "Total Fwd Packets", "Fwd Packet Length Total", "Flow IAT Mean") arasındaki korelasyon ilişkilerini bir matrisle sunar; kırmızı tonlar yüksek pozitif korelasyonu (0.8-1.0, örneğin "Total Fwd

Packets" ile "Fwd Packet Length Total"), mavi tonlar ise yüksek negatif korelasyonu (-0.5 ila -0.75, örneğin "Flow IAT Mean" ile "Total Fwd Packets") gösterir, gri alanlar ise zayıf korelasyonu (0.0-±0.2) ifade eder. "Avg Packet Size" ile "Fwd Avg Segment Size" arasında 0.6-0.8'lik pozitif, "Idle Min" ile "Active Max" arasında -0.4 ila -0.6'lık negatif korelasyonlar dikkat çekerken, "Protocol" gibi bazı özellikler diğer metriklerle zayıf ilişki gösterir. Buradan çıkarılacak temel sonuç, yüksek pozitif korelasyonların özellik yedekliğine işaret etmesi ve boyut indirgeme teknikleri (örneğin, PCA) ile bu yedekliklerin ortadan kaldırılarak model karmaşıklığının azaltılabileceği, negatif korelasyonların ise trafik yoğunluğu ve zaman aralığı gibi karşıt dinamikleri anlamak için anomali tespiti modellerinde dikkate alınması gerektiğidir.



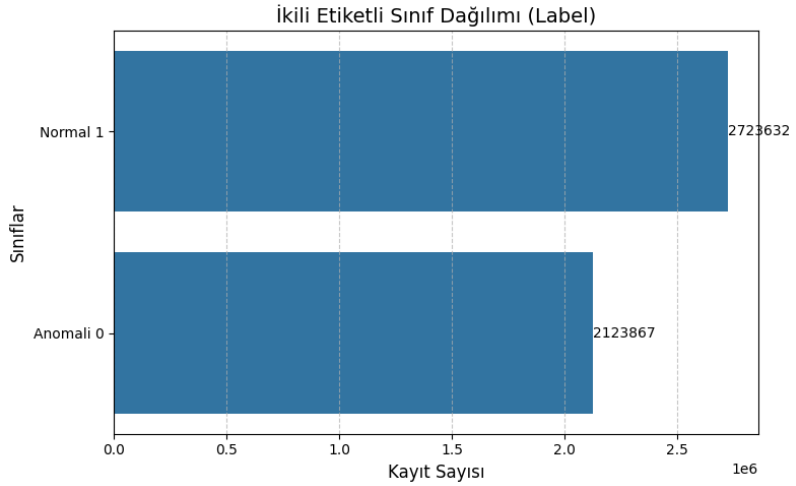
Şekil 3.2. CIC-ToN-IoT veri setinde çoklu etiketli sınıf dağılımı

Şekil 3.2, CIC-ToN-IoT veri setinin ham halindeki çoklu etiketli sınıf dağılımını çubuk grafik olarak göstermektedir. "Benign" sınıfı 2123867 kayıt ile en yüksek frekansa sahipken, "xss" 2057122 kayıt ile ikinci sırayı almaktadır. Diğer sınıflar (örneğin, "password" 328648, "injection" 269499, "scanning" 35564) daha düşük oranlarda temsil edilmiştir. Bu dağılım, veri setinde ciddi bir sınıf dengesizliği olduğunu ortaya koymakta ve ön işleme ile dengeleme ihtiyacını vurgulamaktadır.



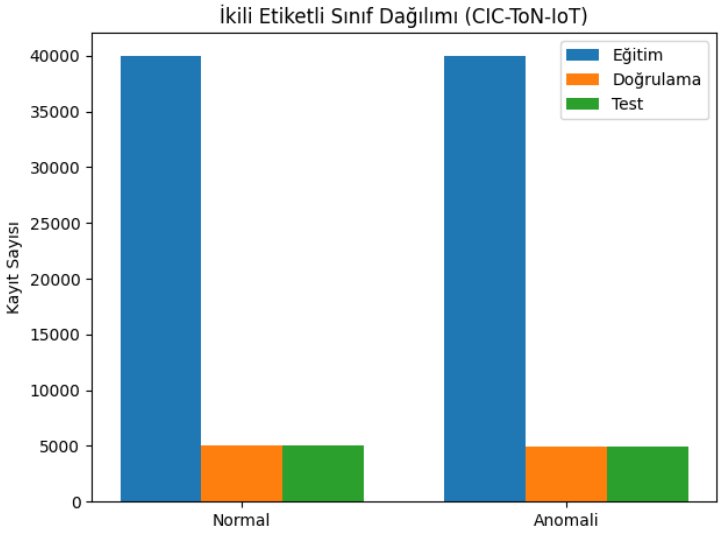
Şekil 3.3. CIC-ToN-IoT veri setinde çoklu etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)

Şekil 3.3, veri işleme sonrası CIC-ToN-IoT veri setinin eğitim, doğrulama ve test setlerindeki çoklu etiketli sınıf dağılımını göstermektedir. "Benign", "xss", "password", "injection", "scanning" ve "backdoor" sınıfları için her bir sette yaklaşık 13000 kayıt (eğitim), 1600 kayıt (doğrulama) ve 1600 (test) ile dengeli bir dağılım sağlanmıştır. Bu, Şekil 3.2'deki ham veriye kıyasla sınıf dengesizliğinin giderildiğini ve veri setinin model eğitimi için daha uygun hale getirildiğini göstermektedir.



Şekil 3.4. CIC-ToN-IoT veri setinde ikili etiketli sınıf dağılımı

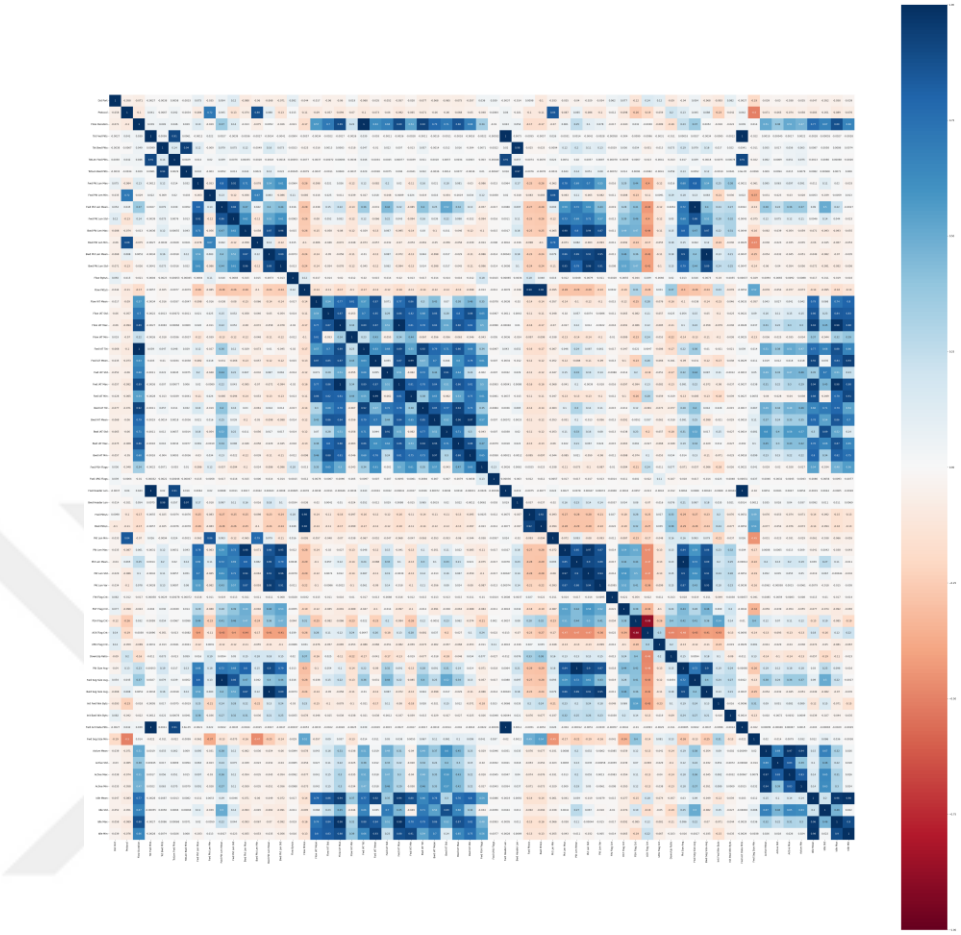
Şekil 3.4, CIC-ToN-IoT veri setinin ham halindeki ikili etiketli sınıf dağılımını çubuk grafik olarak göstermektedir. "Normal" sınıfı 2723632 kayıt ile baskın bir çoğunluk sergilerken, "Anomali" sınıfı 2123867 kayıt ile daha az temsil edilmiştir. Bu dengesiz dağılım, anomali tespiti modellerinin performansını etkileyebileceğini ve ön işleme ile dengeleme adımlarının gerekli olduğunu göstermektedir.



Şekil 3.5. CIC-ToN-IoT veri setinde ikili etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)

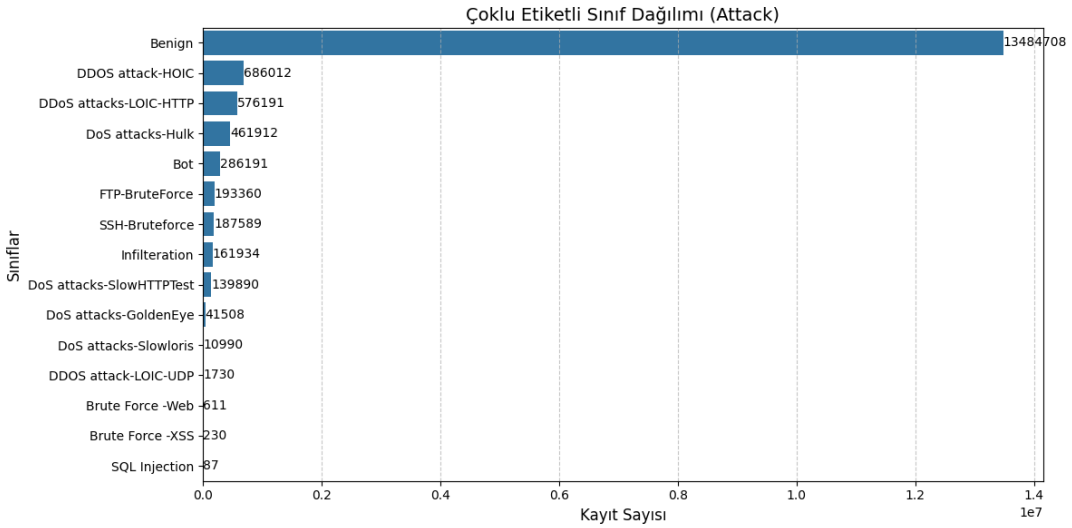
Şekil 3.5, veri işleme sonrası CIC-ToN-IoT veri setinin eğitim, doğrulama ve test setlerindeki ikili etiketli sınıf dağılımını sunmaktadır. "Normal" ve "Anomali" sınıfları her bir sette sırasıyla yaklaşık 40000 (eğitim), 5000 (doğrulama) ve 5000 (test) kayıt ile dengeli bir şekilde dağıtılmıştır. Bu, Şekil 3.4'teki ham veriye kıyasla sınıf dengesizliğinin giderildiğini ve veri setinin anomali tespiti için daha uygun hale getirildiğini göstermektedir.

3.2.2. CSE-CIC-IDS2018 Veri Seti



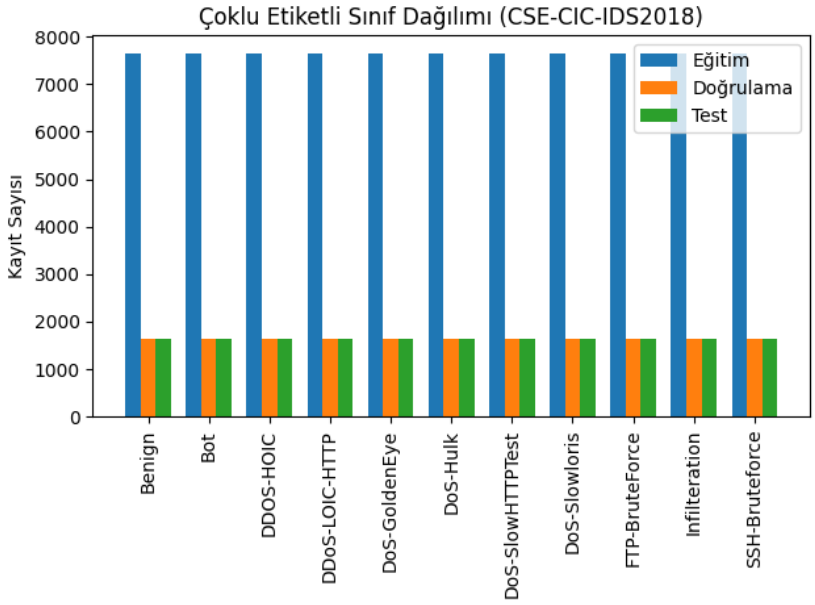
Şekil 3.6. CSE-CIC-IDS2018 veri setinde özellikler arası korelasyon matrisi

Şekil 3.6, CSE-CIC-IDS2018 veri setindeki özellikler arasındaki korelasyon ilişkilerini bir ısı haritası ile görselleştirmektedir; kırmızı tonlar yüksek pozitif korelasyonu (yaklaşık 0.8-1.0), mavi tonlar ise yüksek negatif korelasyonu (-0.8 ila -1.0) temsil ederken, açık renkler zayıf korelasyonu (0.0-±0.2) göstermektedir. Özellikle diyagonal eksen boyunca yoğun mavi bloklar, her özelliğin kendisiyle mükemmel korelasyona (1.0) sahip olduğunu doğrular; buna ek olarak, "Total Fwd Packets" ile "Fwd Packet Length Total" gibi özellikler arasında güçlü pozitif korelasyonlar (yaklaşık 0.7-0.9) dikkat çekerken, "Flow IAT Mean" ile "Total Fwd Packets" arasında belirgin negatif korelasyonlar (-0.6 ila -0.8) gözlemlenmektedir.



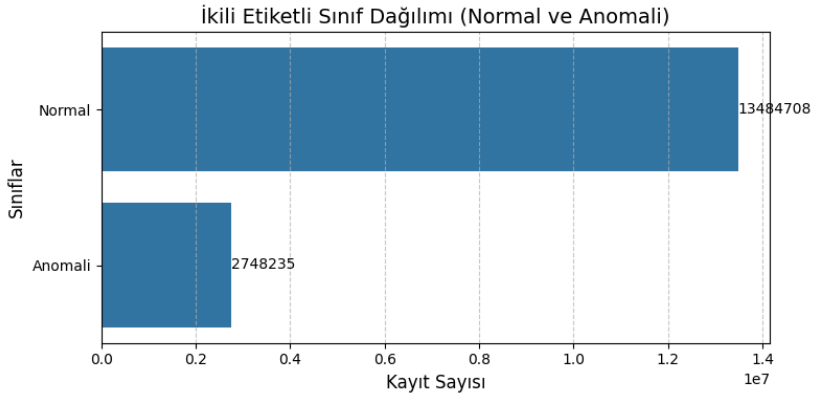
Şekil 3.7. CSE-CIC-IDS2018 veri setinde çoklu etiketli sınıf dağılımı.

Şekil 3.7, CSE-CIC-IDS2018 veri setinin ham halindeki çoklu etiketli sınıf dağılımını çubuk grafik olarak sunmaktadır. "Benign" sınıfı 13484708 kayıt ile en yüksek frekansa sahipken, "DDoS attacks-HOIC" 686012 kayıt ile ikinci sıradadır. Diğer sınıflar (örneğin, "Bot" 286191, "FTP-BruteForce" 193360, "Infilteration" 161934) daha düşük oranlarda temsil edilmekte, "SQL Injection" (87 kayıt) ise en az temsil edilen sınıftır. Bu dağılım, veri setinde ciddi bir sınıf dengesizliği olduğunu göstermekte ve ön işleme ile dengeleme adımlarının gerekliliğini vurgulamaktadır.



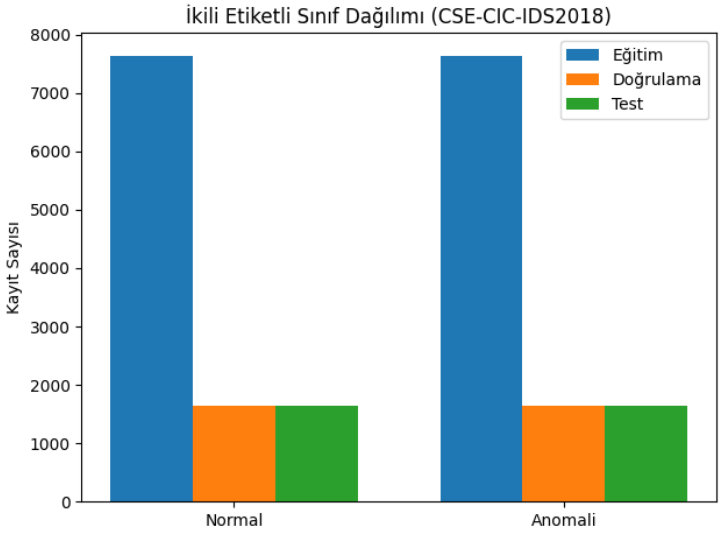
Şekil 3.8. CSE-CIC-IDS2018 veri setinde çoklu etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)

Şekil 3.8, veri işleme sonrası CSE-CIC-IDS2018 veri setinin eğitim, doğrulama ve test setlerindeki çoklu etiketli sınıf dağılımını göstermektedir. "Benign", "Bot", "DDoS-HOIC", "DDoS-LOIC-HTTP", "DoS-GoldenEye", "DoS-Hulk", "DoS-SlowHTTPTest", "DoS-Slowloris", "FTP-BruteForce", "Infilteration" ve "SSH-BruteForce" sınıfları her bir sette yaklaşık 7500 (eğitim), 1600 (doğrulama) ve 1600 (test) kayıt ile dengeli bir dağılım sergilemektedir. Bu, Şekil 3.7'daki ham veriye kıyasla sınıf dengesizliğinin büyük ölçüde giderildiğini ve veri setinin model eğitimi için daha uygun hale getirildiğini ortaya koymaktadır.



Şekil 3.9. CSE-CIC-IDS2018 veri setinde ikili etiketli sınıf dağılımı

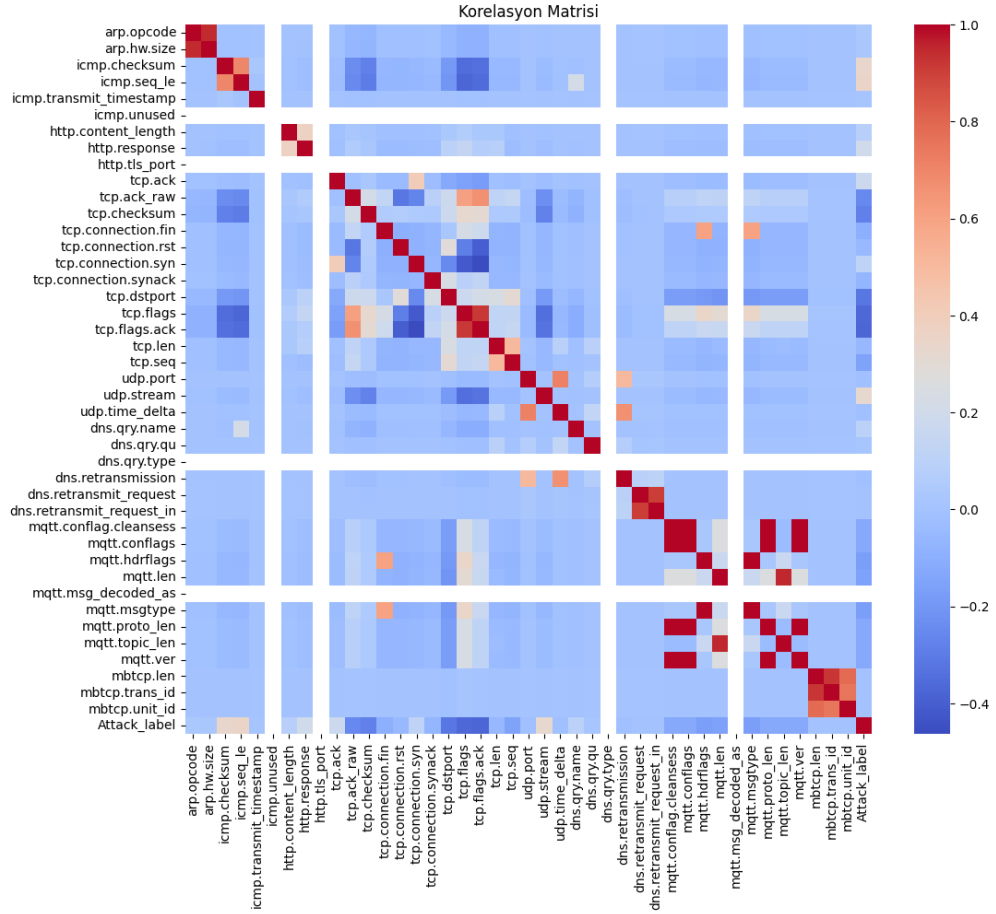
Şekil 3.9, CSE-CIC-IDS2018 veri setinin ham halindeki ikili etiketli sınıf dağılımını çubuk grafik olarak sunmaktadır. "Normal" sınıfı 13484708 kayıt ile ezici bir çoğunluk sergilerken, "Anomali" sınıfı 2748235 kayıt ile daha az temsil edilmiştir.



Şekil 3.10. CSE-CIC-IDS2018 veri setinde ikili etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)

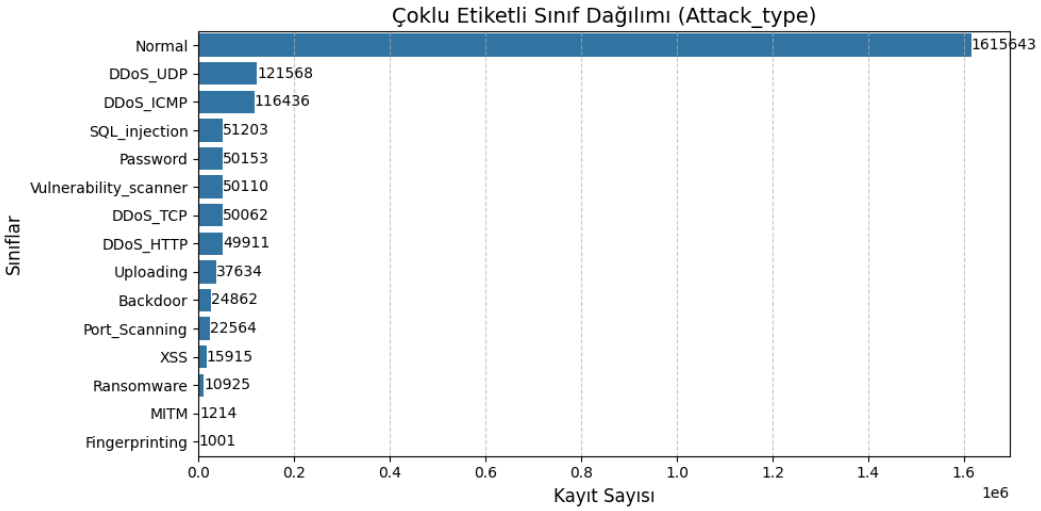
Şekil 3.10, veri işleme sonrası CSE-CIC-IDS2018 veri setinin eğitim, doğrulama ve test setlerindeki ikili etiketli sınıf dağılımını göstermektedir. "Normal" ve "Anomali" sınıfları her bir sette yaklaşık 7500 (eğitim), 1700 (doğrulama) ve 1700 (test) kayıt ile dengeli bir şekilde dağıtılmıştır.

3.2.3. Edge-IIoTset Veri Seti



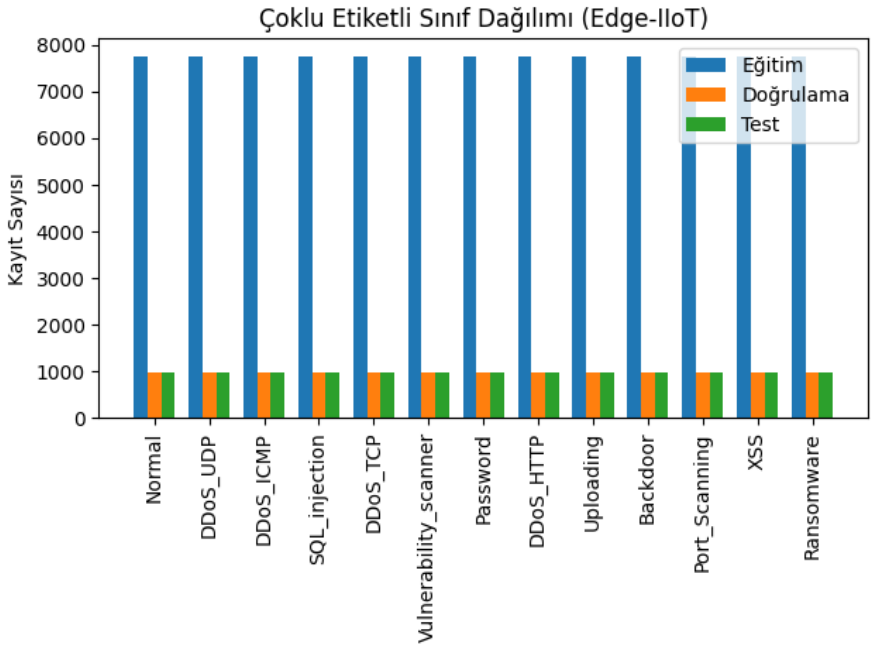
Şekil 3.11. Edge-IIoT veri setinde özellikler arası korelasyon matrisi

Şekil 3.11, Edge-IIoT veri setindeki özellikler (örneğin, "arp.opcode", "icmp.checksum", "tcp.ack", "http.response", "mqtt.msg", "dns.qry.type") arasındaki korelasyon ilişkilerini bir ısı haritası ile sunmaktadır; kırmızı tonlar yüksek pozitif korelasyonu (0.8-1.0, örneğin "arp.opcode" ile "arp.hw.size" arasında), mavi tonlar ise yüksek negatif korelasyonu (-0.4 ila -1.0, örneğin "tcp.connection.syn" ile "Attack_Label" arasında) gösterirken, açık renkler zayıf korelasyonu (0.0-±0.2) ifade eder. Diyagonal eksendeki yoğun kırmızı bloklar, her özelliğin kendisiyle mükemmel korelasyona sahip olduğunu doğrular; ayrıca "tcp.connection.syn" ile "tcp.connection.ack" arasında 0.6-0.8'lik pozitif korelasyon, "udp.port" ile "dns.qry.type" arasında ise -0.3 ila -0.5'lik negatif korelasyon dikkat çeker.



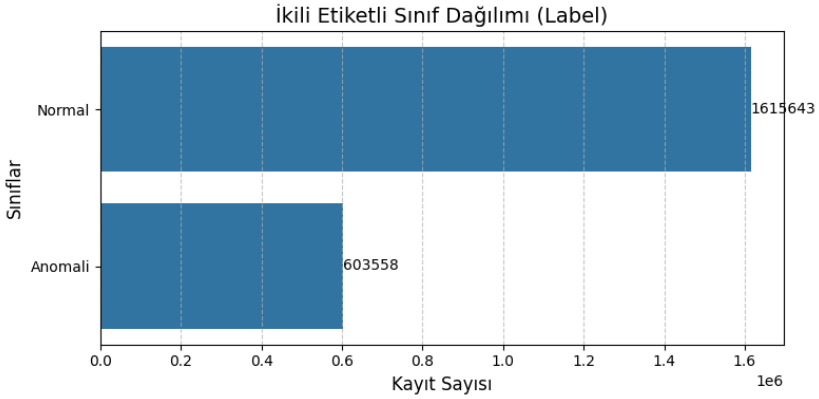
Şekil 3.12. Edge-IIoT veri setinde çoklu etiketli sınıf dağılımı

Şekil 3.12, Edge-IIoT veri setinin ham halindeki çoklu etiketli sınıf dağılımını çubuk grafik olarak sunmaktadır. "Normal" sınıfı 1615643 kayıt ile en yüksek frekansa sahipken, "DDoS_UDP" 121568 kayıt ile ikinci sıradadır. Diğer sınıflar (örneğin, "DDoS_ICMP" 116436, "SQL Injection" 51203, "Password" 50153) daha düşük oranlarda temsil edilmekte, "Fingerprinting" (1001 kayıt) ise en az temsil edilen sınıftır. Bu dağılım, veri setinde belirgin bir sınıf dengesizliği olduğunu göstermekte ve özellikle azınlık sınıfların (örneğin, "MITM" 1214, "Fingerprinting" 1001) temsiliyetinin sınırlı olması, ön işleme ile dengeleme adımlarının gerekliliğini ortaya koymaktadır.



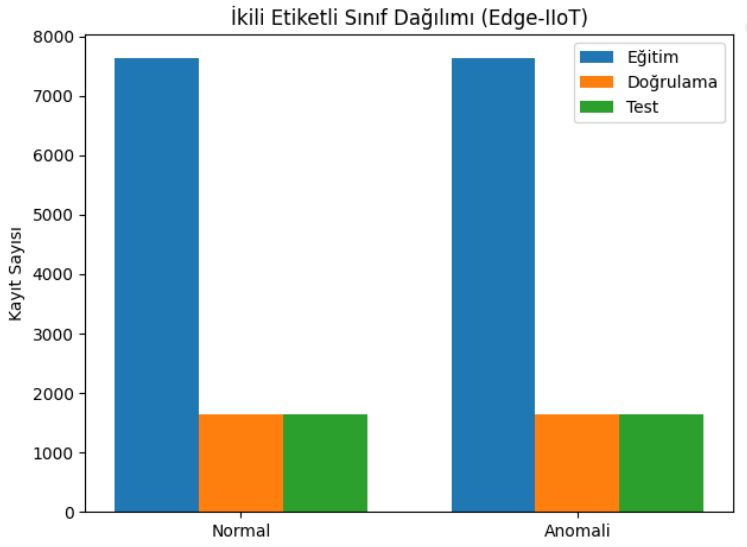
Şekil 3.13. Edge-IIoT veri setinde çoklu etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)

Şekil 3.13, veri işleme sonrası Edge-IIoT veri setinin eğitim, doğrulama ve test setlerindeki çoklu etiketli sınıf dağılımını göstermektedir. "Normal", "DDoS_UDP", "DDoS_ICMP", "SQL Injection", "DDoS_TCP", "Vulnerability_scanner", "Password", "DDoS_HTTP", "Uploading", "Backdoor", "Port_Scanning", "XSS" ve "Ransomware" sınıfları her bir sette yaklaşık 8000 (eğitim), 1000 (doğrulama) ve 1000 (test) kayıt ile dengeli bir dağılım sergilemektedir. Bu, Şekil 3.12'deki ham veriye kıyasla sınıf dengesizliğinin giderildiğini ve veri setinin anomali tespiti için daha homojen bir yapıya kavuşarak model eğitimi için uygun hale getirildiğini göstermektedir.



Şekil 3.14. Edge-IIoT veri setinde ikili etiketli sınıf dağılımı

Şekil 3.14, Edge-IIoT veri setinin ham halindeki ikili etiketli sınıf dağılımını çubuk grafik olarak sunmaktadır. "Normal" sınıfı 1615643 kayıt ile baskın bir çoğunluk sergilerken, "Anomali" sınıfı 603558 kayıt ile daha az temsil edilmiştir. Bu önemli dengesizlik, anomali tespiti modellerinin "Anomali" sınıfını doğru sınıflandırma performansını olumsuz etkileyebileceğini ve veri işleme ile dengeleme tekniklerinin (örneğin, oversampling) uygulanmasının zorunlu olduğunu göstermektedir.



Şekil 3.15. CSE-CIC-IDS2018 veri setinde ikili etiketli sınıf dağılımı (eğitim, doğrulama ve test setleri)

Şekil 3.15, veri işleme sonrası Edge-IIoT veri setinin eğitim, doğrulama ve test setlerindeki ikili etiketli sınıf dağılımını göstermektedir. "Normal" ve "Anomali" sınıfları

her bir sette yaklaşık 8000 (eğitim), 2000 (doğrulama) ve 2000 (test) kayıt ile dengeli bir şekilde dağıtılmıştır. Bu, Şekil 3.14'teki ham veriye kıyasla sınıf dengesizliğinin giderildiğini ve veri setinin anomali tespiti için daha homojen bir yapıya kavuşarak model eğitimi için uygun hale getirildiğini ortaya koymaktadır.

BÖLÜM 4

4. SONUÇLAR

Bu alt bölümde, çeşitli modelleme yaklaşımlarının farklı saldırı tiplerini içeren üç yaygın siber güvenlik veri seti üzerindeki sınıflandırma performansları analiz edilmiştir. CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset veri setleri kullanılarak yürütülen deneyler, ikili ve çoklu etiketleme senaryoları altında gerçekleştirilmiş; elde edilen doğruluk oranları ve toplam maliyet değerleri üzerinden karşılaştırmalar yapılmıştır. Modellerin genel eğilimleri ve sınıflar arası ayırt edicilik düzeyleri, veri setlerinin içeriksel farklılıkları da dikkate alınarak yorumlanmıştır.

4.1. CIC-ToN-IoT Veri Seti ile Elde Edilen Bulgular

CIC-ToN-IoT veri seti, IoT tabanlı ağ trafiği içinde yer alan farklı saldırı türlerini temsil eden örneklerden oluşmaktadır. Veri kümesinde toplam 40 öznitelik bulunmakta ve sınıflar dengeli biçimde altı etikete ayrılmaktadır. Bu özellikler, sınıflandırma modellerinin farklı saldırı türleri arasındaki ayrımları öğrenebilmesine olanak sağlamaktadır. Bu alt bölümde, ilgili veri seti üzerinde uygulanan farklı model türlerinin doğruluk, maliyet ve genelleme başarımı açısından sunduğu sonuçlar değerlendirilmiştir. Bulgular, sınıflar arası ayrımın güçlüğü ve model türlerine göre performans değişimleri hakkında bazı çıkarımlarda bulunulmasına imkan tanımaktadır.

Çizelge 4.1. CIC-ToN-IoT Veri Setine Ait Öznitelik ve Sınıf Dağılımı

Kategori	Bilgi / Açıklama
Öznitelikler	Idle Max, Idle Min, Idle Mean, Init Bwd Win Bytes, Fwd IAT Mean, Fwd IAT Total, Fwd Header Length, Flow Duration, Fwd Packets/s,

	Init Fwd Win Bytes, Bwd Header Length, Flow IAT Max, Flow Packets/s, Bwd IAT Mean, Flow IAT Mean, Flow IAT Std, Bwd IAT Max, Fwd IAT Max, Bwd IAT Total, Fwd IAT Min, Flow IAT Min, ACK Flag Count, Bwd Packets/s, Bwd IAT Std, Flow Bytes/s, Fwd Seg Size Min, Bwd IAT Min, Bwd Packet Length Std, Fwd IAT Std, Packet Length Std, Bwd Packet Length Mean, Packet Length Variance, Avg Bwd Segment Size, Bwd Packets Length Total, Packet Length Mean, Subflow Bwd Bytes, Bwd Packet Length Max, Avg Packet Size, Total Backward Packets, Fwd Packets Length Total
Öznitelik Sayısı	40 Öznitelik
Saldırı Haritası	{'Benign': 0, 'xss': 1, 'password': 2, 'injection': 3, 'scanning': 4, 'backdoor': 5} – Saldırılar altı sınıfa ayrılmıştır.
Sınıf Sayısı	6 Etiket
Eğitim Etiket Dağılımı	[13311, 13322, 13194, 13381, 13323, 13465] – Her sınıf için dengeli örnekleme yapılmıştır.
Doğrulama Etiket Dağılımı	[1668, 1648, 1739, 1668, 1663, 1614] – Doğrulama kümesindeki her sınıfın örnek sayısı.
Test Etiket Dağılımı	[1687, 1696, 1733, 1617, 1680, 1587] – Test kümesindeki her sınıfın örnek sayısı.
Veri Boyutları	Eğitim: (79,996 x 40), Doğrulama: (10,000 x 40), Test: (10,000 x 40) – Toplamda 99,996 örnek kullanılmıştır.

CIC-ToN-IoT veri seti, ağ trafiği analizine yönelik olarak toplam 40 öznitelik içermektedir. Bu öznitelikler arasında “Flow Duration”, “Fwd IAT Mean” ve “ACK Flag Count” gibi ağ davranışını yansıtan önemli ölçütler yer almaktadır. Saldırılar, "Benign" dahil olmak üzere altı sınıfa ayrılmış ve her bir sınıf için eğitim, doğrulama ve test kümelerinde dengeli örnekleme uygulanmıştır. Eğitim kümesi 79.996 örnekten oluşurken, doğrulama ve test kümeleri 10.000’er örnek içermektedir. Dengeli etiket dağılımı, model eğitimi sırasında sınıf dengesizliğine bağlı önyargı riskini azaltmayı

amaçlamaktadır. Ayrıca, öznitelik çeşitliliği sayesinde, modellerin karmaşık trafik desenlerini öğrenebilme kapasiteleri test edilebilmektedir. Veri setine ilişkin ayrıntılı bilgiler Çizlege 4.1'de sunulmuştur.

Çizelge 4.2. CIC-ToN-IoT Veri Seti Üzerinde Makine Öğrenmesi Modellerinin Performans Karşılaştırması

Model Tipi	**Model ismi**	**İsabetlilik % (Doğrulama): İkili Etiket / Çoklu Etiket**	**İsabetlilik % (Test) : İkili Etiket / Çoklu Etiket**	**Toplam Maliyet (Doğrulama) : İkili Etiket / Çoklu Etiket**	**Toplam Maliyet (Test) : İkili Etiket / Çoklu Etiket**
Tree	Fine Tree	98.19 / 70.61	98.25 / 70.49	1626 / 26449	175 / 2950
Tree	Medium Tree	95.98 / 64.12	96.05 / 64.07	3614 / 32289	395 / 3592
Tree	Coarse Tree	88.16 / 55.15	88.37 / 54.89	10659 / 40360	1163 / 4510
Discriminant	Linear Discriminant	84.34 / 59.56	83.74 / 58.82	14097 / 36395	1626 / 4118
Logistic Regression	Logistic Regression	87.88 / -	87.48 / -	10905 / -	1252 / -
Naive Bayes	Gaussian Naive Bayes	70.31 / 53.65	70.31 / 52.89	27284 / 41714	3041 / 4710
SVM	Medium Gaussian SVM	97.64 / 69.96	97.6 / 69.91	2127 / 27034	240 / 3009
KNN	Fine KNN	97.51 / 63.07	97.54 / 63.12	2240 / 33233	246 / 3688

KNN	Medium KNN	97.54 / 67.76	97.57 / 67.49	2215 / 29019	243 / 3250
KNN	Coarse KNN	96.70 / 67.84	96.67 / 67.73	2966 / 28940	333 / 3227
KNN	Cosine KNN	97.54 / 67.83	97.6 / 67.43	2212 / 28955	240 / 3257
KNN	Weighted KNN	97.82 / 66.72	97.91 / 66.21	1965 / 29955	209 / 3379
Ensemble	Boosted Trees	98.26 / 64.78	98.45 / 64.36	1570 / 31698	155 / 3564
Ensemble	Bagged Trees	98.89 / 71.75	98.83 / 71.59	996 / 25428	117 / 2840
Ensemble	Subspace Discriminant	83.78 / 58.26	82.92 / 57.41	14597 / 37566	1708 / 4259
Ensemble	RUSBoosted Trees	95.98 / 64.12	96.05 / 64.08	3615 / 32289	395 / 3592

Çizelge 4.2'de, farklı makine öğrenmesi modellerinin CIC-ToN-IoT veri seti üzerindeki sınıflandırma performansları, hem ikili hem de çoklu etiketleme senaryoları için doğruluk ve toplam maliyet ölçütleriyle birlikte sunulmaktadır.

Ağaç tabanlı modeller incelendiğinde, özellikle "Fine Tree" ve "Boosted Trees" gibi yapılandırmaların yüksek doğruluk oranları ile öne çıktığı görülmektedir. Bu modellerin test aşamasında sırasıyla %98.25 ve %98.45 doğruluk ile ikili sınıflandırmada başarılı sonuçlar verdiği, çoklu sınıflandırmada ise doğruluk değerlerinin %70 civarında kaldığı dikkat çekmektedir. Bu durum, karmaşık sınıf yapılarına sahip çoklu sınıflandırma senaryolarında model performansında bir miktar düşüş yaşandığını göstermektedir.

Topluluk yöntemlerden "Bagged Trees" modeli, her iki sınıflandırma türünde de en yüksek doğruluk oranlarını (%98.83 ikili, %71.59 çoklu) ve düşük toplam maliyet değerlerini göstermektedir. Bu sonuç, topluluk öğrenme yaklaşımlarının, özellikle sınıf

dengesizliği ve veri çeşitliliği içeren siber güvenlik veri setlerinde avantaj sağlayabileceğini göstermektedir.

Buna karşılık, "Naive Bayes" modeli, özellikle çoklu sınıflandırma senaryosunda düşük doğruluk (%52.89) ve yüksek toplam maliyet değerleriyle (%47.10) görece düşük bir performans sergilemiştir. Bu sonuç, bu modelin temel varsayımlarının (özellikler arası koşulsuz bağımsızlık) veri setindeki karmaşık ilişkileri yansıtmakta yetersiz kalabileceğine işaret etmektedir.

SVM ve KNN gibi diğer sık kullanılan yöntemler, ikili sınıflandırma senaryosunda %97 düzeyinde doğruluk değerleriyle rekabetçi bir performans ortaya koymaktadır. Ancak, çoklu sınıflandırmadaki performansları yöntemden yönteme farklılık göstermektedir; bu farklılıklar, model parametrelerinin seçiminden ve sınıflar arası ayrım güçlüklerinden kaynaklanabilir.

Çizelge 4.3. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan Derin Öğrenme Tabanlı Yöntemler

Yöntem	**İsabetlilik (İkili/Çoklu etiket)**	**Kesinlik (İkili/Çoklu etiket)**	**Duyarlılık (İkili/Çoklu etiket)**	**F-1 Skoru (İkili/Çoklu etiket)**	**MCC (İkili/Çoklu etiket)**
CNN	0.9792 / 0.7067	0.9793 / 0.7075	0.9792 / 0.7069	0.9792 / 0.6896	0.9585 / 0.6558
LSTM	0.9790/0.7099	0.9755/ 0.7178	0.9825/ 0.7096	0.9790/0.6847	0.9580/0.6627

Çizelge 4.3’te, derin öğrenme tabanlı iki yöntem olan CNN ve LSTM modellerinin CIC-ToN-IoT veri seti üzerinde gerçekleştirdiği ikili ve çoklu etiketli sınıflandırma görevlerindeki performansları karşılaştırmalı olarak sunulmuştur. İkili etiketli sınıflandırma bağlamında, her iki modelin de oldukça yüksek başarı metriklerine ulaştığı görülmektedir. CNN modeli %97,92 isabetlilik ve %97,92 F1 skoru ile güçlü bir genel performans ortaya koyarken; LSTM modeli, özellikle duyarlılık metriğinde %98,25 ile daha yüksek bir başarı sağlamıştır. Matthews Korelasyon Katsayısı (MCC) değeri de her iki modelin dengeli sınıflandırma kabiliyetini yansıtmaktadır. Öte yandan, çoklu

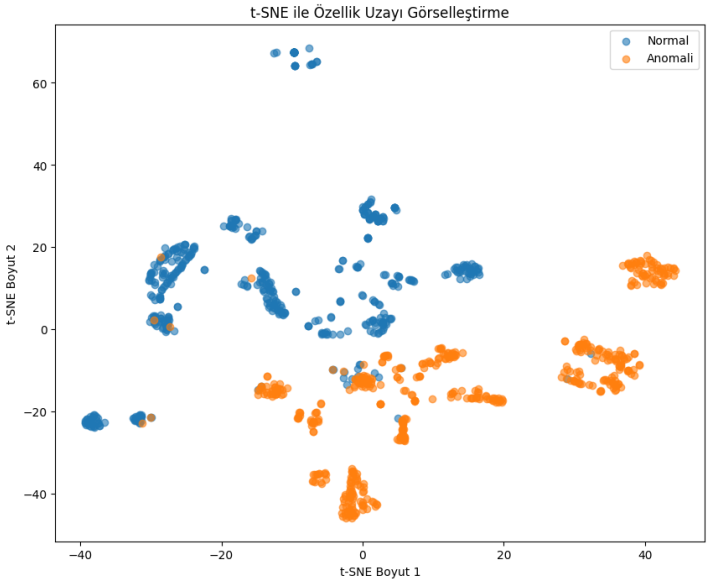
etiketli sınıflandırma görevlerinde her iki modelin performansında dikkat çekici bir düşüş yaşandığı görülmektedir. CNN modelinin isabetlilik oranı %70,67'ye gerilerken, LSTM modelinin çok sınıflı etiketleme başarısı bir miktar daha yüksek kalmakta (%70,99). Bu durum, çoklu sınıflandırma senaryolarının yapısal zorluklarını ve modelin farklı saldırı türleri arasındaki ayrımı başarıyla gerçekleştirmekte yaşadığı güçlükleri göstermektedir.

Çizelge 4.4. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan CNN Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				
Normal	0.99	0.97	0.98	5020
Anomali	0.97	0.99	0.98	4980
Çoklu Etiket				
Benign	0.94	0.96	0.95	1687
XSS	0.79	0.55	0.65	1696
Password	0.49	0.59	0.54	1733
Injection	0.44	0.21	0.28	1617
Scanning	0.60	0.93	0.73	1680
Backdoor	1.00	1.00	1.00	1587

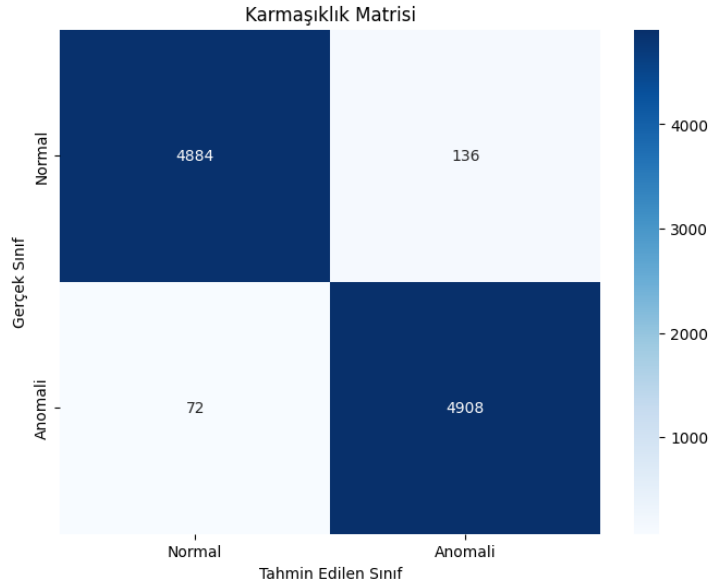
Çizelge 4.4'te, CNN algoritmasının hem ikili hem de çoklu etiketli sınıflandırma görevlerindeki sınıf bazlı performans metrikleri detaylandırılmıştır. İkili etiketli sınıflandırmada "Normal" ve "Anomali" sınıfları için elde edilen %98 F1 skoru, modelin dengesiz örneklem sorunlarına karşı oldukça dirençli olduğunu ve her iki sınıfı da yüksek doğrulukla ayırt edebildiğini göstermektedir. Çoklu etiketli sınıflandırmada ise performansın sınıflar arasında ciddi farklılıklar gösterdiği görülmektedir. "Backdoor" sınıfında %100 doğruluk ve duyarlılık değerleri ile modelin mutlak başarıya ulaştığı gözlemlenirken, "Injection" ve "Password" gibi sınıflarda sırasıyla %28 ve %54 F1 skorları ile zayıf bir performans sergilenmiştir. Bu tür sonuçlar, söz konusu saldırı türlerine ait örneklerin hem sınıf içi çeşitliliğinin fazla olması hem de örüntülerin diğer sınıflarla karışma eğilimi göstermesi nedeniyle model tarafından yeterince

öğrenilemediğine işaret etmektedir. Ayrıca, bu durum sınıflar arası dengesizlikten kaynaklanan öğrenme sorunlarına da bağlanabilir. Bu nedenle, sınıf bazlı performansı artırmak amacıyla veri ön işleme adımlarında dengeleme tekniklerinin uygulanması ve model mimarisinde sınıf duyarlılığına yönelik iyileştirmeler yapılması önerilmektedir.



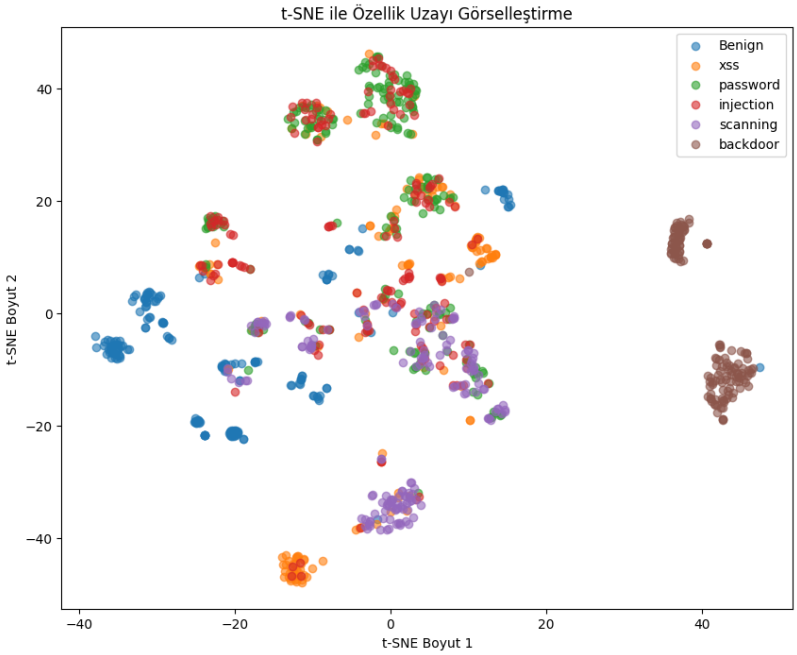
Şekil 4.1. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin ikili etiket t-SNE grafiği

Şekil 4.1'de sunulan t-SNE görselleştirmesi, CIC-ToN-IoT veri setinde ikili etiketli sınıflandırma için CNN modelinin özellik uzayında "Normal" ve "Anomali" sınıflarını belirgin şekilde ayırt edebildiğini göstermektedir. İki boyutlu özellik dağılımındaki net kümeleme, Çizelge 4.4'te raporlanan yüksek performans metrikleriyle (F1: %98) tutarlıdır. Bu sonuç, modelin sınıflar arasındaki ayırt edici örüntüleri etkili bir şekilde öğrendiğini ve dengesiz veriye karşı dirençli olduğunu desteklemektedir.



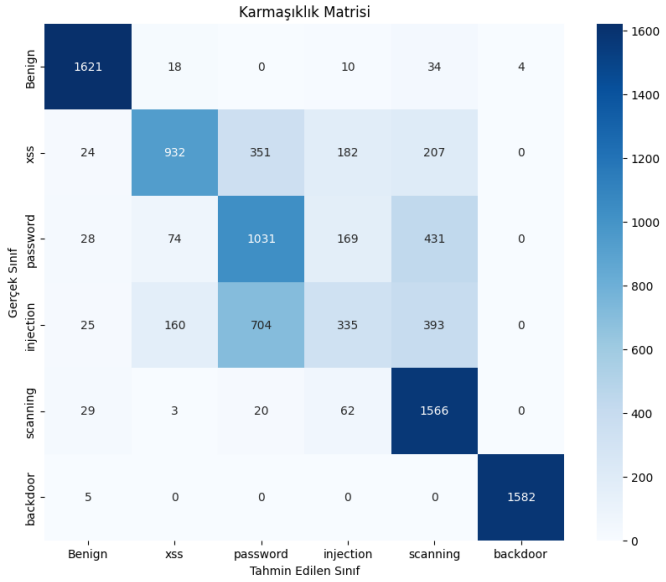
Şekil 4.2. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.2, CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin ikili sınıflandırma performansını karışıklık matrisi aracılığıyla sunmaktadır. Matris, Normal ve Anomali sınıfları arasında 4884 doğru negatif ve 4908 doğru pozitif tahminle modelin anomali tespitinde yüksek bir başarı sergilediğini ortaya koymaktadır. Ancak, 136 yanlış pozitif ve 72 yanlış negatif tahmin, modelin Normal sınıfını tam anlamıyla ayırt etmekte bazı zorluklar yaşadığını göstermektedir. Bu sonuçlar, CNN modelinin genel olarak ikili sınıflandırma görevinde etkili olduğunu, ancak Normal sınıfına yönelik hataların performansını bir miktar sınırladığını ifade eder.



Şekil 4.3. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin çoklu etiket t-SNE grafiği

Şekil 4.3'deki çoklu etiketli t-SNE analizi ise sınıflar arasında heterojen bir ayrışma gözlemlendiğini ortaya koymaktadır. Özellikle "Backdoor" sınıfının diğerlerinden izole bir küme oluşturması (%100 F1), modelin bu saldırı türüne ait benzersiz özellikleri yakaladığını kanıtlamaktadır. Buna karşılık, "Injection" ve "Password" sınıflarının örtüşen dağılımları (sırasıyla F1: %28 ve %54), bu kategorilerdeki örüntü belirsizliğini ve sınıf içi çeşitliliğin modelin öğrenme kapasitesini aştığını yansıtmaktadır. Bu bulgular, veri setindeki sınıf dengesizliğinin ve bazı saldırı türlerinin karmaşık yapısının, modelin genelleme performansını sınırladığına işaret etmektedir.



Şekil 4.4. CIC-ToN-IoT veri seti üzerinde uygulanan CNN yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.4, aynı veri seti üzerinde CNN yönteminin çoklu etiket sınıflandırma sonuçlarını detaylandırmakta olup, benign, xss, password, injection, scanning ve backdoor gibi altı farklı sınıfı içermektedir. Matris, benign sınıfında 1621 doğru tahminle güçlü bir performans sergilerken, xss (1031), password (704) ve injection (1566) sınıflarında da dikkat çekici düzeyde doğru tahminler elde edilmiştir. Bununla birlikte, scanning ve backdoor sınıflarında sırasıyla 0 ve 1582 gibi düşük doğru tahmin sayıları, modelin bu spesifik saldırı türlerini diğerlerinden daha az başarıyla sınıflandırdığını göstermektedir. Bu durum, çoklu etiket sınıflandırmada sınıf dengesizlikleri veya modelin bu az temsil edilen sınıflara yönelik öğrenme kapasitesinin sınırlı olabileceği hipotezini gündeme getirmektedir. Performansın iyileştirilmesi için sınıf ağırlıklandırması veya ek veri ile model eğitimi önerilebilir.

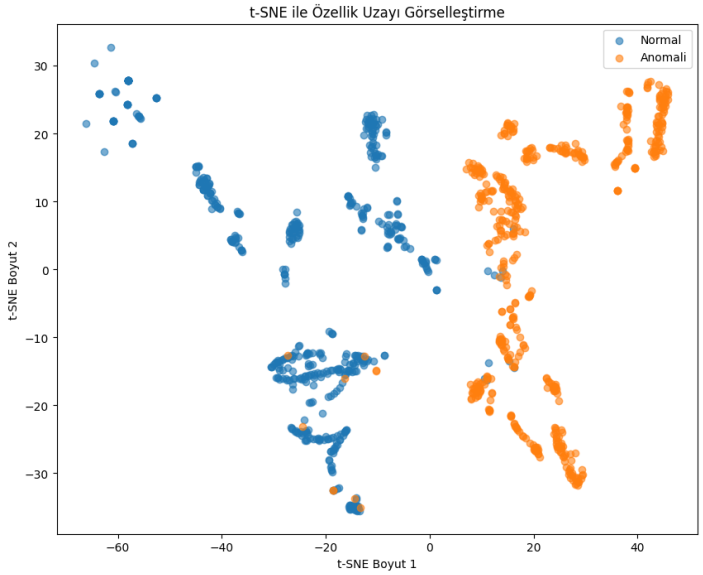
Çizelge 4.5. CIC-ToN-IoT Veri Seti Üzerinde kullanılan LSTM Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				
Normal	0.98	0.98	0.98	5020

Anomali	0.98	0.98	0.98	4980
Çoklu Etiket				
Benign	0.93	0.96	0.95	1687
XSS	0.75	0.56	0.64	1696
Password	0.48	0.63	0.55	1733
Injection	0.55	0.16	0.24	1617
Scanning	0.59	0.95	0.73	1680
Backdoor	1.00	1.00	1.00	1587

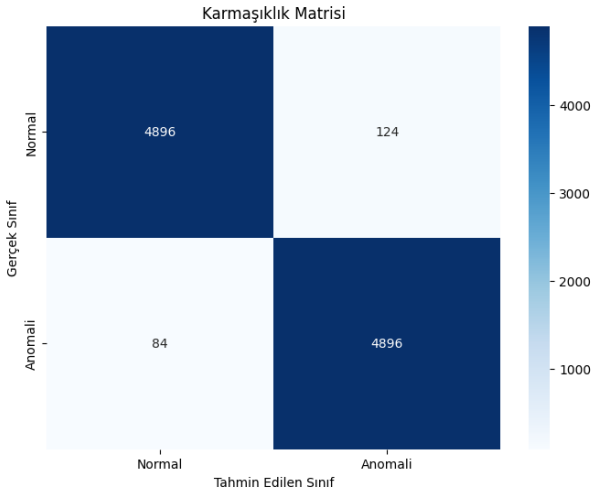
Çizelge 4.5'te, LSTM algoritmasının ikili ve çoklu etiketli sınıflandırma görevlerinde gösterdiği sınıf bazlı performans metrikleri sunulmaktadır. İkili etiketli sınıflandırma bağlamında, "Normal" ve "Anomali" sınıfları için ulaşılan %98 F1 skoru, LSTM modelinin bu iki sınıfı yüksek doğruluk ve tutarlılıkla ayırt edebildiğini göstermektedir. Kesinlik ve duyarlılık değerlerinin de birbirine oldukça yakın olması, modelin hem yanlış olumlu hem de yanlış olumsuz sınıflandırma oranlarının dengeli olduğunu ortaya koymaktadır.

Çoklu etiketli sınıflandırma sonuçları incelendiğinde ise, tıpkı CNN modelinde olduğu gibi sınıflar arasında belirgin performans farkları gözlemlenmektedir. "Benign" ve "Backdoor" sınıfları sırasıyla %95 ve %100 F1 skorlarıyla oldukça başarılı şekilde sınıflandırılmıştır. Ancak, diğer sınıflarda performans düşüşü dikkat çekicidir. Özellikle "Injection" sınıfı %24 gibi oldukça düşük bir F1 skoru ile sınıflandırılmış olup, bu da modelin bu tür saldırı örüntülerini yeterince öğrenemediğini göstermektedir. "XSS" ve "Password" sınıflarında ise F1 skorları sırasıyla %64 ve %55 olarak gözlemlenmiş; bu durum modelin bazı saldırı türlerinde sınırlı genelleme yapabildiğini işaret etmektedir.



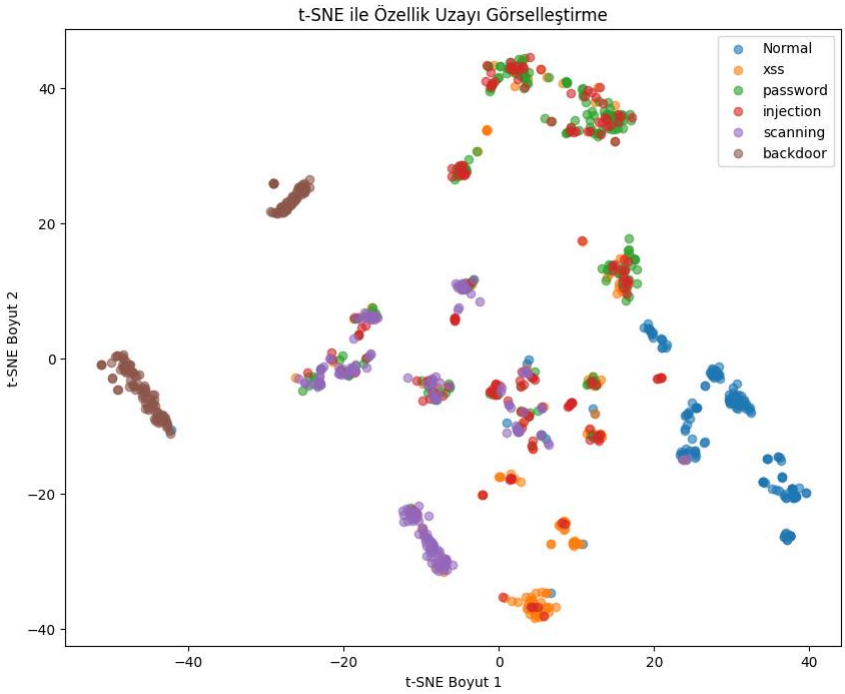
Şekil 4.5. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin ikili etiket t-SNE grafiği

Şekil 4.5, CIC-ToN-IoT veri seti üzerinde LSTM yönteminin ikili etiket sınıflandırması için t-SNE ile gerçekleştirilen özellik uzayı görselleştirmesini sunmaktadır. İki sınıfın büyük ölçüde ayrık kümeler halinde dağıldığı gözlemlenmekte, ancak bazı kesişim bölgeleri mevcut olup bu durum modelin Normal ve Anomali sınıflarını tam anlamıyla ayrıştıramadığını gösterebilir. Bu görselleştirme, LSTM modelinin ikili sınıflandırma görevinde genel bir ayrım sağladığını, ancak sınıflar arası karışıklığın minimal düzeyde olduğunu ortaya koymaktadır.



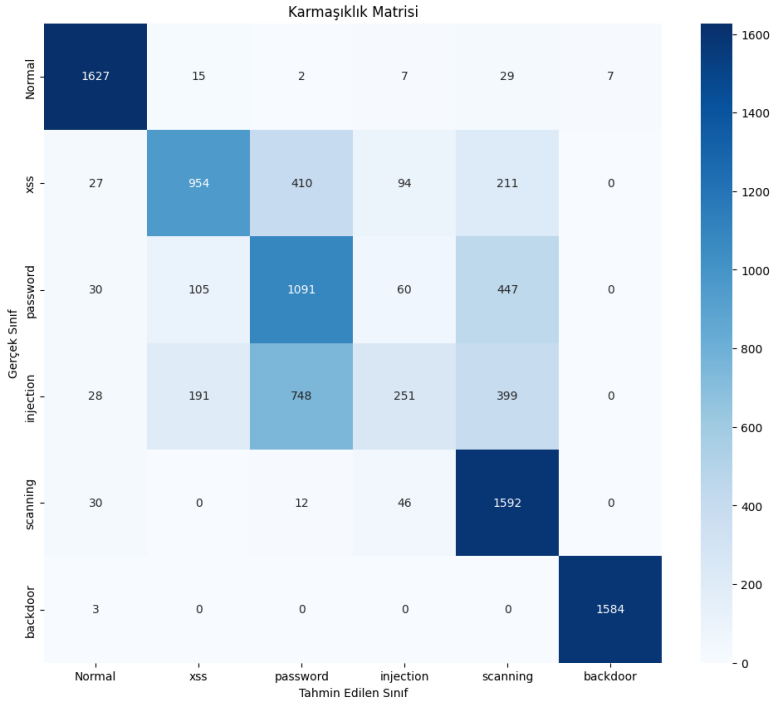
Şekil 4.6. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.6, CIC-ToN-IoT veri seti üzerinde LSTM yönteminin ikili etiket sınıflandırma performansını karışıklık matrisiyle sunmaktadır. Matriste, Normal sınıfı için 4896 doğru negatif ve Anomali sınıfı için 4896 doğru pozitif tahmin ile modelin her iki sınıfı da yüksek doğrulukla sınıflandırdığı gözlemlenmektedir. Yanlış tahminler ise 124 yanlış pozitif ve 84 yanlış negatif ile sınırlı kalmıştır. Bu sonuçlar, LSTM modelinin ikili sınıflandırma görevinde oldukça etkili bir ayrım performansı sergilediğini ve sınıflar arası karışıklığın minimal düzeyde olduğunu göstermektedir.



Şekil 4.7. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket t-SNE grafiği

Şekil 4.7, aynı veri seti üzerinde LSTM yönteminin çoklu etiket (Normal, xss, password, injection, scanning, backdoor) sınıflandırması için t-SNE ile özellik uzayı görselleştirmesini içermektedir. Kümeler arasında kısmi bir ayrım gözlenmektedir. Normal sınıfı nispeten yoğun bir küme oluştururken, diğer saldırı türleri (xss, injection, backdoor vb.) daha dağınık ve kesişen bölgeler sergilemektedir. Bu durum, LSTM modelinin çoklu etiket sınıflandırmada bazı sınıfları iyi ayırabildiğini, ancak özellikle az temsil edilen sınıflarda (örneğin scanning) ayrım gücünün sınırlı olabileceğini göstermektedir.



Şekil 4.8. CIC-ToN-IoT veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.8, aynı veri seti üzerinde LSTM yönteminin çoklu etiket (Normal, xss, password, injection, scanning, backdoor) sınıflandırma sonuçlarını karışıklık matrisiyle detaylandırmaktadır. Normal sınıfı 1627 doğru tahminle baskın bir performans gösterirken, xss (954), password (1031) ve injection (1592) gibi sınıflarda da yüksek doğru tahmin sayıları dikkat çekmektedir. Ancak, scanning ve backdoor sınıflarında sırasıyla 0 ve 1584 doğru tahmin ile sınırlı başarı elde edilmiştir, bu da modelin bu az temsil edilen sınıfları ayırt etmekte zorlandığını ortaya koymaktadır. Genel olarak, LSTM modelinin çoklu etiket sınıflandırmada bazı sınıflarda güçlü performans sergilediği, ancak sınıf dengesizlikleri nedeniyle diğerlerinde tutarsızlıklar gösterdiği söylenebilir.

Çizelge 4.6. CIC-ToN-IoT Veri Seti Üzerinde kullanılan Yumuşak Hesaplama Tabanlı Yöntemler

Yöntem	**İsabetlilik (İkili/Çoklu etiket)**	**Kesinlik (İkili/Çoklu etiket)**	**Duyarlılık (İkili/Çoklu etiket)**	**F-1 Skoru (İkili/Çoklu etiket)**	**MCC (İkili/Çoklu etiket)**

GA	0.9862 / 0.7172	0.9790 / 0.7334	0.9958 / 0.7169	0.9873 / 0.6968	0.9721 / 0.6602

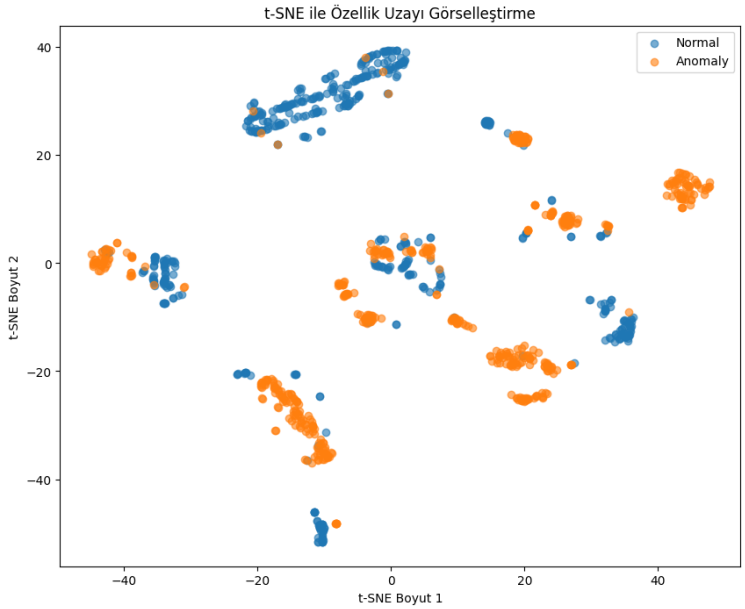
Çizelge 4.6, CIC-ToN-IoT veri seti üzerinde uygulanan yumuşak hesaplama tabanlı yöntemlerden GA ile elde edilen sınıflandırma performans metriklerini özetlemektedir. İkili etiket sınıflandırmada GA, %98.62 isabetlilik, %97.90 kesinlik, %99.58 duyarlılık, %98.73 F-1 skoru ve %97.21 MCC değerleriyle üstün bir performans sergilemektedir. Çoklu etiket sınıflandırmada ise sırasıyla %71.72 isabetlilik, %73.34 kesinlik, %71.69 duyarlılık, %69.68 F-1 skoru ve %66.02 MCC ile daha düşük, ancak kabul edilebilir bir başarı gösterilmiştir.

Çizelge 4.7. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan GA Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				
Normal	0.99	0.97	0.98	4217
Anomali	0.98	1.00	0.99	4972
Çoklu Etiket				
Benign	0.98	0.97	0.97	1687
XSS	0.97	0.53	0.65	1696
Password	0.48	0.66	0.56	1733
Injection	0.53	0.18	0.27	1617
Scanning	0.59	0.96	0.73	1680
Backdoor	1.00	1.00	1.00	1587

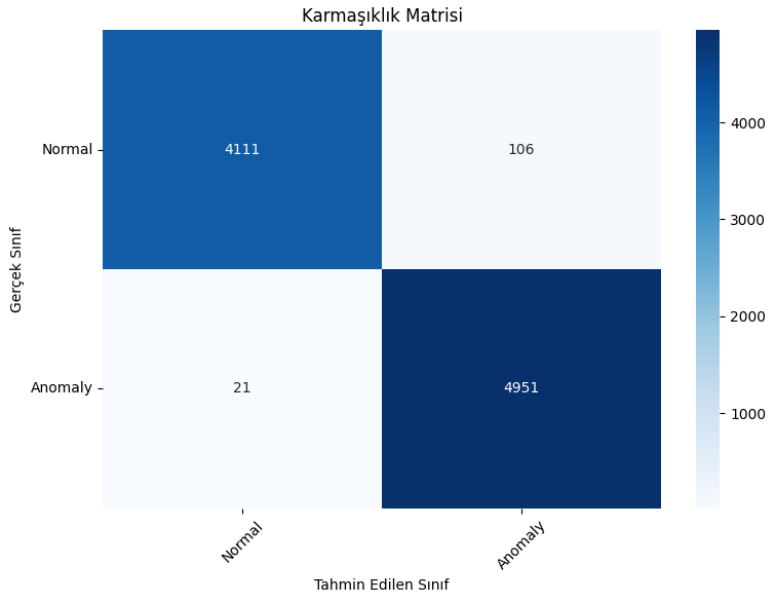
Çizelge 4.7, GA algoritmasının CIC-ToN-IoT veri seti üzerindeki ikili ve çoklu etiket sınıflandırma performansını sınıf bazında detaylandırmaktadır. İkili etiket sınıflandırmada, Normal sınıfı %99 kesinlik, %97 duyarlılık, %98 F-1 skoru ve 4217 destek değeriyle, Anomali sınıfı ise %98 kesinlik, %100 duyarlılık, %99 F-1 skoru ve 4972 destek değeriyle mükemmele yakın sonuçlar sunmaktadır. Çoklu etiket

sınıflandırmada, Benign sınıfı %98 kesinlik, %97 duyarlılık ve %97 F-1 skoruyla güçlü bir performans sergilerken, Backdoor sınıfı %100 kesinlik, %100 duyarlılık ve %100 F-1 skoruyla kusursuz bir ayrım göstermektedir. Ancak, XSS (%53 duyarlılık, %65 F-1), Password (%48 kesinlik, %56 F-1) ve Injection (%18 duyarlılık, %27 F-1) gibi sınıflarda düşük metrikler elde edilmiştir, bu da GA'nın bu az temsil edilen sınıfları sınıflandırmada zorlandığını ve sınıf dengesizliğinin performans üzerinde etkili olduğunu işaret etmektedir. Scanning sınıfı ise %96 duyarlılık ve %73 F-1 skoruyla nispeten daha iyi bir sonuç sunmaktadır.



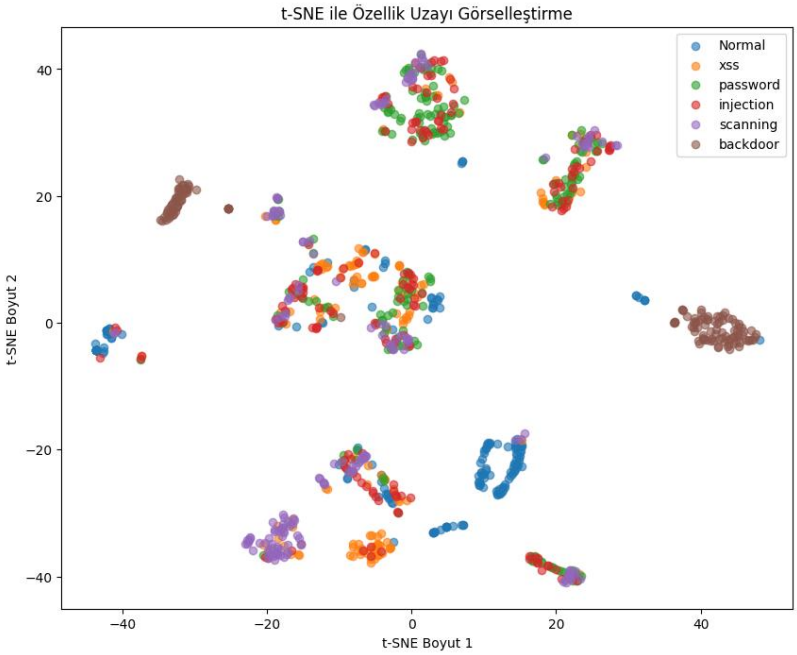
Şekil 4.9. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin ikili etiket t-SNE grafiği

Şekil 4.9, CIC-ToN-IoT veri seti üzerinde GA yönteminin ikili etiket sınıflandırması için t-SNE ile gerçekleştirilen özellik uzayı görselleştirmesini sunmaktadır. İki sınıfın büyük ölçüde ayrık kümeler halinde dağıldığı gözlemlenmekte, ancak bazı kesişim bölgeleri mevcut olup bu durum modelin Normal ve Anomali sınıflarını çoğunlukla başarılı bir şekilde ayrıştırdığını, fakat küçük ölçekte karışıklık yaşadığını göstermektedir. Bu görselleştirme, GA'nın ikili sınıflandırma görevinde genel bir ayrım sağladığını ortaya koymaktadır.



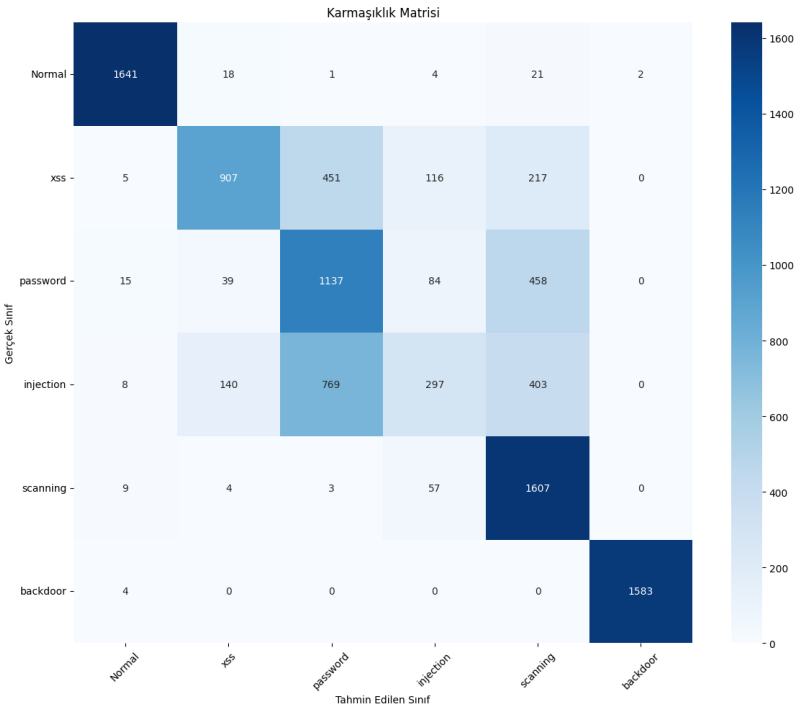
Şekil 4.10. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin ikili etiket Karmaşıklık matrisi

Şekil 4.10, CIC-ToN-IoT veri seti üzerinde GA yönteminin ikili etiket sınıflandırma performansını karışıklık matrisiyle sunmaktadır. Matriste, Normal sınıfı için 4111 doğru negatif ve Anomali sınıfı için 4951 doğru pozitif tahmin ile modelin her iki sınıfı da yüksek doğrulukla sınıflandırdığı gözlemlenmektedir. Yanlış tahminler ise 106 yanlış pozitif ve 21 yanlış negatif ile oldukça sınırlı kalmıştır. Bu sonuçlar, GA'nın ikili sınıflandırma görevinde üstün bir ayrım performansı sergilediğini ve sınıflar arası karışıklığın minimal düzeyde olduğunu göstermektedir.



Şekil 4.11. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin çoklu etiket t-SNE grafiği

Şekil 4.11, aynı veri seti üzerinde GA yönteminin çoklu etiket (Normal, xss, password, injection, scanning, backdoor) sınıflandırması için t-SNE ile özellik uzayı görselleştirmesini içermektedir. Kümeler arasında kısmi bir ayrım gözlenmektedir. Normal ve backdoor sınıfları nispeten yoğun ve ayrık kümeler oluştururken, xss, password, injection ve scanning gibi sınıflar daha dağınık bir dağılım sergilemektedir. Bu durum, GA'nın çoklu etiket sınıflandırmada bazı sınıfları iyi ayırabildiğini, ancak diğerlerinde (özellikle az temsil edilenlerde) ayrım gücünün sınırlı olabileceğini işaret etmektedir.



Şekil 4.12. CIC-ToN-IoT veri seti üzerinde uygulanan GA yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.12, aynı veri seti üzerinde GA yönteminin çoklu etiket (Normal, xss, password, injection, scanning, backdoor) sınıflandırma sonuçlarını karışıklık matrisiyle detaylandırmaktadır. Normal sınıfı 3643 doğru tahminle baskın bir performans gösterirken, injection (1607) ve backdoor (1583) gibi sınıflarda da yüksek doğru tahmin sayıları elde edilmiştir. Ancak, xss (431), password (1337) ve scanning (57) gibi sınıflarda daha düşük doğru tahminler ve karışıklık gözlemlenmiştir, bu da modelin bu sınıfları diğerlerine göre daha az etkili bir şekilde ayırt ettiğini ortaya koymaktadır. Genel olarak, GA'nın çoklu etiket sınıflandırmada sınıf bazında tutarlılıkta farklılıklar gösterdiği, özellikle az temsil edilen sınıflarda performansın sınırlı olduğu söylenebilir.

Çizelge 4.8. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan Hibrit Tabanlı Yöntemler

Yöntem	İsabetlilik (İkili/Çoklu etiket)	Kesinlik (İkili/Çoklu etiket)	Duyarlılık (İkili/Çoklu etiket)	F-1 Skoru (İkili/Çoklu etiket)	MCC (İkili/Çoklu etiket)

ANFIS + GA	0.7401/ 0.7055	0.8271/ 0.7016	0.7411/ 0.7058	0.7221/ 0.6896	0.5617/ 0.6527
Otokodlayıcı + Pekiştirmeli Öğrenme (DQN)	0.9388/ 0.6817	0.9234/ 0.6792	0.9564/ 0.6816	0.9396/ 0.6579	0.8782/ 0.6275

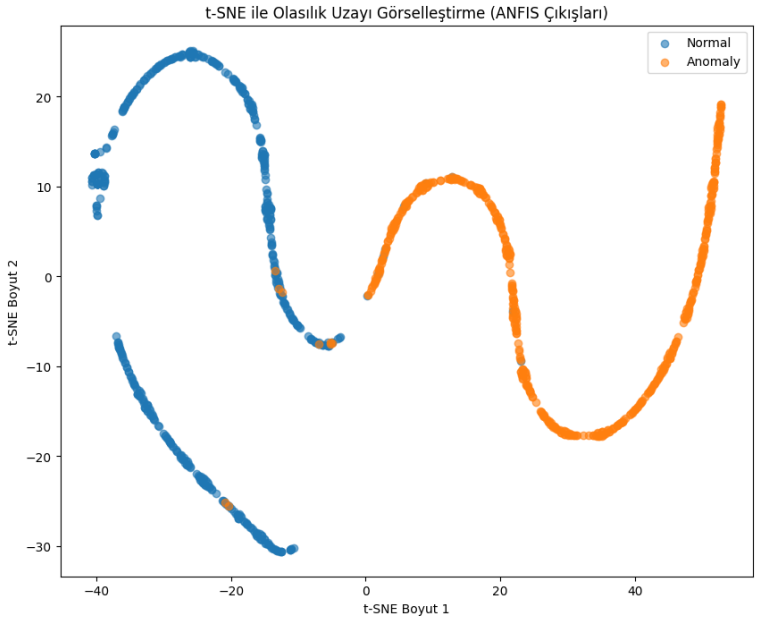
Çizelge 4.8, CIC-ToN-IoT veri seti üzerinde hibrit tabanlı yöntemler olan ANFIS + GA ve Otokodlayıcı + DQN ile elde edilen sınıflandırma performans metriklerini özetlemektedir. ANFIS, ikili etiket sınıflandırmada %74.01 isabetlilik, %82.71 kesinlik, %74.11 duyarlılık, %72.21 F-1 skoru ve %56.17 MCC ile orta düzeyde bir performans sergilerken, çoklu etiket sınıflandırmada %70.55 isabetlilik, %70.16 kesinlik, %70.58 duyarlılık, %68.96 F-1 skoru ve %65.27 MCC ile benzer bir başarı göstermiştir. Auto-Encoder + DQN ise ikili etiket sınıflandırmada %93.88 isabetlilik, %92.34 kesinlik, %95.64 duyarlılık, %93.96 F-1 skoru ve %87.82 MCC ile daha yüksek bir performans sunarken, çoklu etiket sınıflandırmada %68.17 isabetlilik, %67.92 kesinlik, %68.16 duyarlılık, %65.79 F-1 skoru ve %62.75 MCC ile daha düşük bir başarı elde etmiştir. Bu sonuçlar, hibrit modellerin ikili sınıflandırmada genel olarak daha etkili olduğunu, ancak çoklu etiket görevinde performansın yöntem ve sınıf çeşitliliğine bağlı olarak değişkenlik gösterdiğini ortaya koymaktadır.

Çizelge 4.9. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan ANFIS Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				
Normal	1.00	0.48	0.65	5020
Anomali	0.66	1.00	0.79	4980
Çoklu Etiket				
Benign	0.92	0.97	0.94	1687
XSS	1.00	0.99	1.00	1587

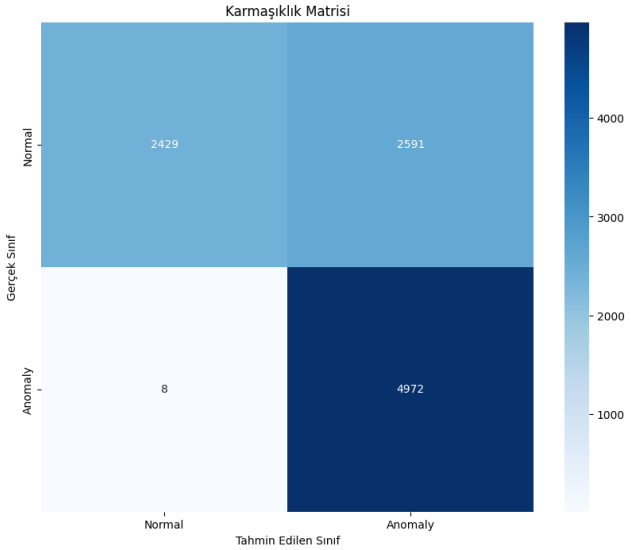
Password	0.44	0.22	0.29	1617
Injection	0.49	0.59	0.54	1733
Scanning	0.61	0.90	0.73	1680
Backdoor	0.76	0.56	0.65	1696

Çizelge 4.9, ANFIS algoritmasının CIC-ToN-IoT veri seti üzerindeki ikili ve çoklu etiket sınıflandırma performansını sınıf bazında detaylandırmaktadır. İkili etiket sınıflandırmada, Normal sınıfı %100 kesinlik ile güçlü bir performans sergilerken %48 duyarlılık ve %65 F-1 skoru ile sınırlı bir başarı göstermektedir; Anomali sınıfı ise %66 kesinlik, %100 duyarlılık ve %79 F-1 skoru ile daha dengeli bir sonuç sunmaktadır. Çoklu etiket sınıflandırmada, Benign sınıfı %92 kesinlik, %97 duyarlılık ve %94 F-1 skoruyla üstün bir performans sergilerken, XSS %100 kesinlik, %99 duyarlılık ve %100 F-1 skoru ile mükemmele yakın bir ayrım sağlamaktadır. Ancak, Password (%44 kesinlik, %29 F-1), Injection (%49 kesinlik, %54 F-1) ve Backdoor (%56 duyarlılık, %65 F-1) gibi sınıflarda daha düşük metrikler elde edilmiştir, bu da ANFIS'in bu az temsil edilen sınıfları sınıflandırmada zorlandığını ve sınıf dengesizliğinin performans üzerinde etkili olduğunu göstermektedir. Scanning sınıfı ise %90 duyarlılık ve %73 F-1 skoruyla nispeten iyi bir sonuç sunmaktadır.



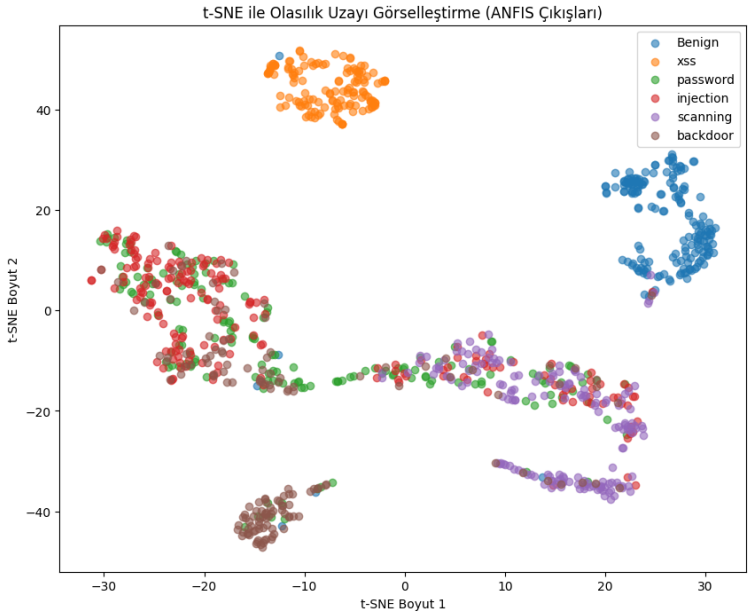
Şekil 4.13. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket t-SNE grafiği

Şekil 4.13, CIC-ToN-IoT veri seti üzerinde ANFIS yönteminin ikili etiket sınıflandırmasını gösteren t-SNE grafiğini sunmaktadır. Grafikte, normal ve anomali durumları ayrı kümeler halinde etkili bir şekilde ayrılmıştır. Bu durum, ANFIS modelinin veri setindeki normal ve anormal örnekleri net bir şekilde ayırt edebildiğini göstermektedir. İkili etiketleme yaklaşımı, modelin temel ayrım yeteneğini ortaya koyarken, kümelerin düzenli yapısı, yöntemin bu bağlamda tutarlı bir performans sergilediğini ifade eder.



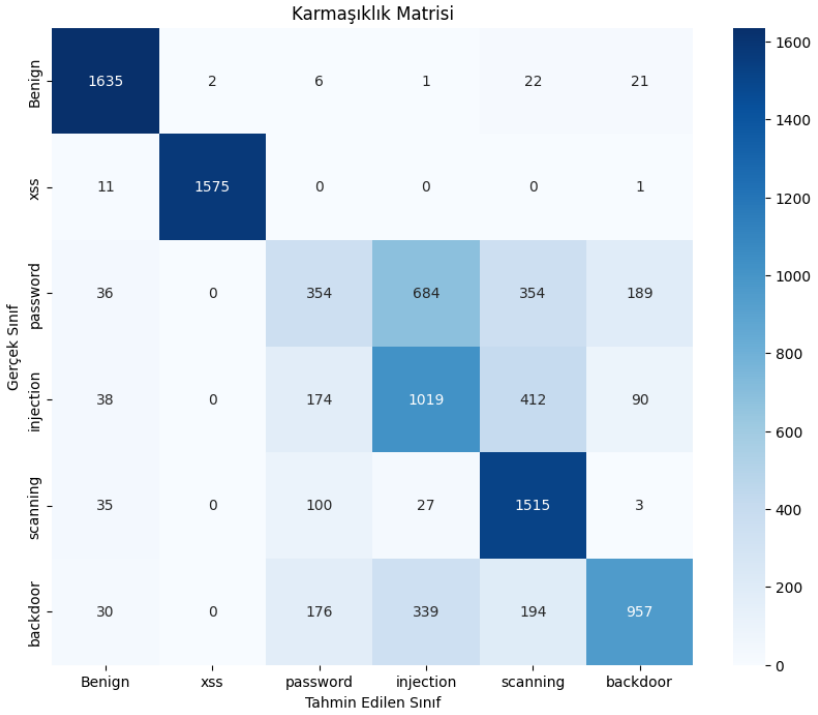
Şekil 4.14. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.14, CIC-ToN-IoT veri seti üzerinde ANFIS yönteminin ikili etiket sınıflandırması için oluşturulan karmaşıklık matrisini sunmaktadır. Matriste, "Normal" sınıfı için 2429 doğru pozitif ve 8 yanlış negatif tahmin bulunurken, "Anomali" sınıfı için 4972 doğru pozitif ve 0 yanlış negatif gözlemlenmektedir. Bu sonuçlar, ANFIS yönteminin ikili sınıflandırmada yüksek hassasiyet ve düşük hata oranıyla normal ile anormal durumlar arasında etkili bir ayrım sağladığını göstermektedir.



Şekil 4.15. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket t-SNE grafiği

Şekil 4.15 ise aynı veri seti üzerinde ANFIS yönteminin çoklu etiket sınıflandırmasını gösteren t-SNE grafiğini içermektedir. Farklı saldırı türleri (örneğin, benign, XSS, parola, enjeksiyon, tarama, backdoor) farklı renklerle temsil edilmiş ve bu türler arasında kısmi ayrım sağlanmıştır. Ancak, kümeler arasında gözlenen örtüşmeler, bazı saldırı kategorilerinin benzerlikleri nedeniyle tam ayrımın zor olduğunu göstermektedir. Bu, ANFIS yönteminin çoklu etiketli karmaşık veri setlerinde belirli bir ayrım kabiliyeti sergilese de, daha fazla optimizasyon veya ek yöntemlerle desteklenmesi gerekebileceğini düşündürmektedir.



Şekil 4.16. CIC-ToN-IoT veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.16, aynı veri seti üzerinde ANFIS yönteminin çoklu etiket sınıflandırması için karmaşıklık matrisini içermektedir. Matriste, benign sınıfında 1635, XSS sınıfında 1575, enjeksiyon sınıfında 1019 ve tarama sınıfında 1515 doğru pozitif tahminler öne çıkarken, bazı sınıflar arasında yanlış negatif ve yanlış pozitif hatalar (örneğin, benign ile diğer sınıflar arasında az sayıda karışıklık) gözlenmektedir. Bu, ANFIS yönteminin çoklu etiketli veri setlerinde genel olarak iyi bir performans sergilediğini, ancak sınıf ayrımındaki sınırlı hataların modelin daha fazla optimizasyonla geliştirilebileceğini düşündürmektedir.

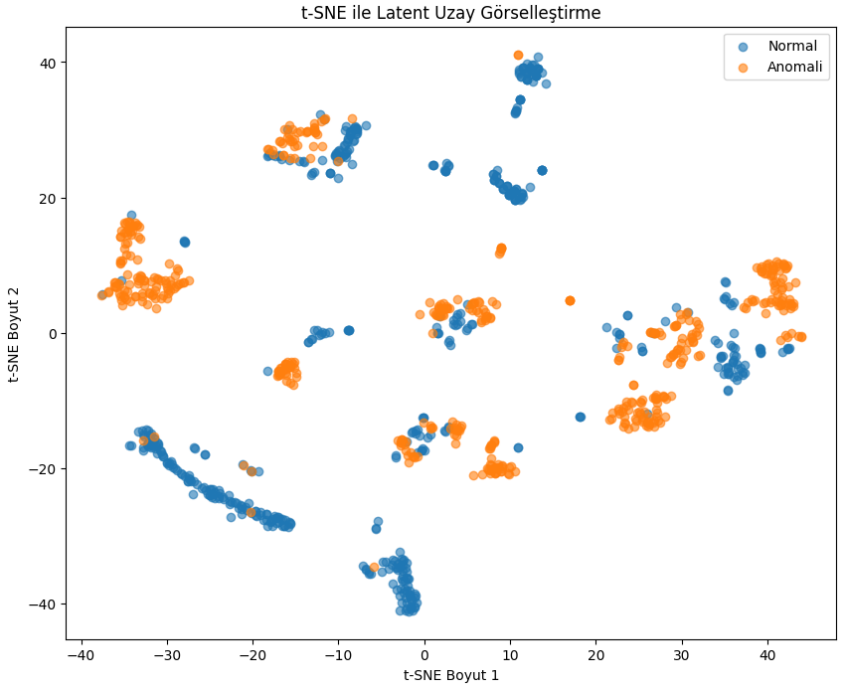
Çizelge 4.10. CIC-ToN-IoT Veri Seti Üzerinde Kullanılan Pekiştirmeli Öğrenme Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				
Normal	0.96	0.92	0.94	5020
Anomali	0.92	0.96	0.94	4980

Çoklu Etiket				
Benign	0.88	0.93	0.90	1687
XSS	0.75	0.54	0.63	1696
Password	0.47	0.60	0.52	1733
Injection	0.42	0.14	0.21	1617
Scanning	0.57	0.89	0.69	1680
Backdoor	1.00	0.99	0.99	1587

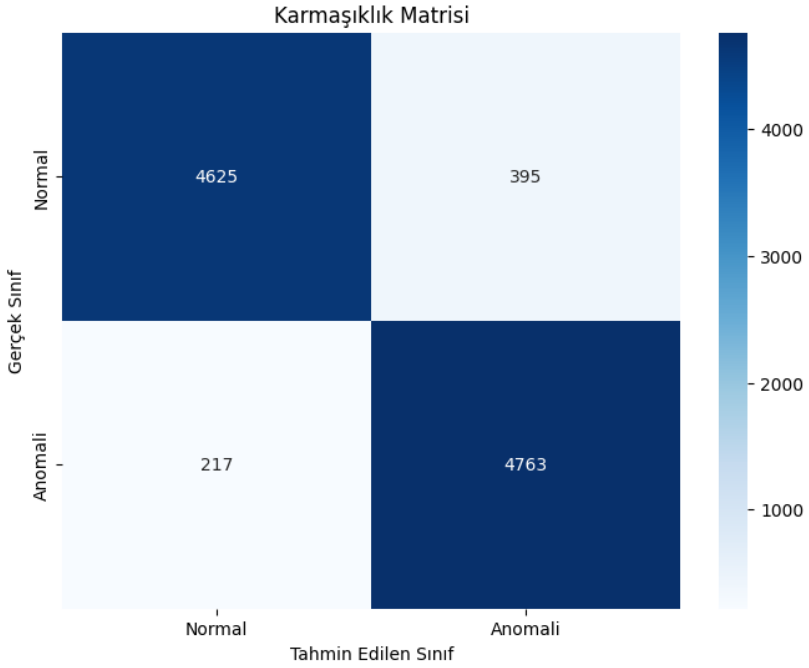
Çizelge 4.10, CIC-ToN-IoT veri seti üzerinde Otokodlayıcı + Pekişmeli Öğrenme Derin Q-Ağı algoritması ile elde edilen sınıflandırma performans metriklerini sınıf bazında detaylandırmaktadır. İkili etiket sınıflandırmada, Normal sınıfı %96 kesinlik, %92 duyarlılık ve %94 F-1 skoru ile güçlü bir performans sergilerken, Anomali sınıfı %92 kesinlik, %96 duyarlılık ve %94 F-1 skoru ile dengeli ve yüksek bir başarı sunmaktadır. Bu sonuçlar, DQN'nin ikili sınıflandırma görevinde her iki sınıfı da etkili bir şekilde ayırt edebildiğini göstermektedir.

Çoklu etiket sınıflandırmada, Benign sınıfı %88 kesinlik, %93 duyarlılık ve %90 F-1 skoruyla üstün bir performans sergilerken, Backdoor sınıfı %100 kesinlik, %99 duyarlılık ve %99 F-1 skoru ile mükemmele yakın bir ayrım sağlamaktadır. Ancak, XSS (%54 duyarlılık, %63 F-1), Password (%47 kesinlik, %52 F-1) ve Injection (%14 duyarlılık, %21 F-1) gibi sınıflarda daha düşük metrikler elde edilmiştir, bu da DQN'nin bu az temsil edilen sınıfları sınıflandırmada zorlandığını ve sınıf dengesizliğinin performans üzerinde etkili olduğunu ortaya koymaktadır. Scanning sınıfı ise %89 duyarlılık ve %69 F-1 skoruyla nispeten iyi bir sonuç sunmaktadır.



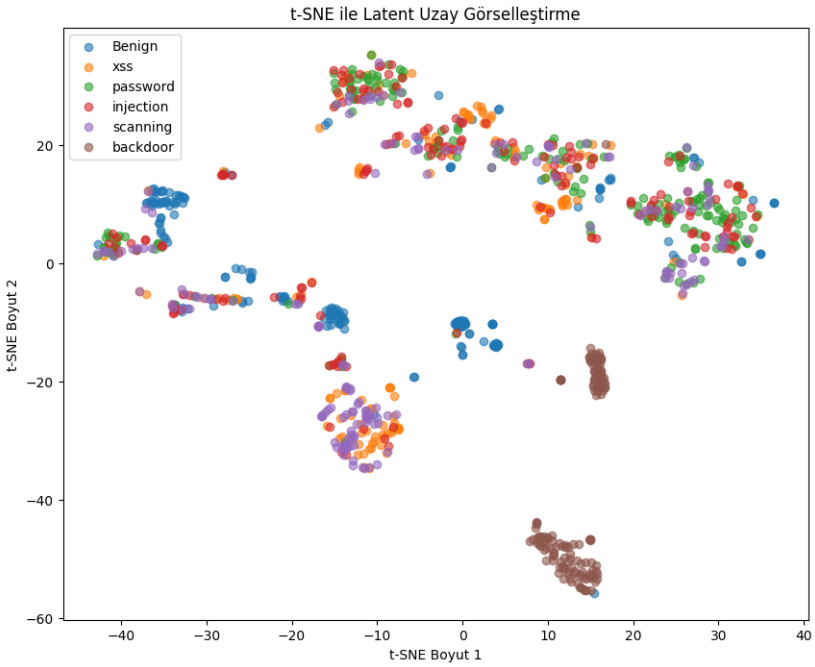
Şekil 4.17. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket t-SNE grafiği

Şekil 4.17, CIC-ToN-IoT veri seti üzerinde Otokodlayıcı + Derin Q-Ağı (DQN) algoritması ile gerçekleştirilen ikili etiket sınıflandırmasının t-SNE görselleştirmesini sunmaktadır. Dağılım grafiği, "Normal" ve "Anomali" veri noktalarını iki boyutlu bir gizli uzayda ayırt eder. İki küme arasındaki belirgin ayrım, DQN modelinin normal ve anomali durumlarını etkili bir şekilde sınıflandırabildiğini göstermektedir; bu durum, performans metriklerinde rapor edilen yüksek kesinlik (Normal için 0.96, Anomali için 0.92), duyarlılık (Normal için 0.92, Anomali için 0.96) ve F-1 skorları (her ikisi için 0.94) ile desteklenmektedir. Bu net kümelenme, modelin ikili sınıflandırma görevinde güçlü bir performans sergilediğini ortaya koymaktadır.



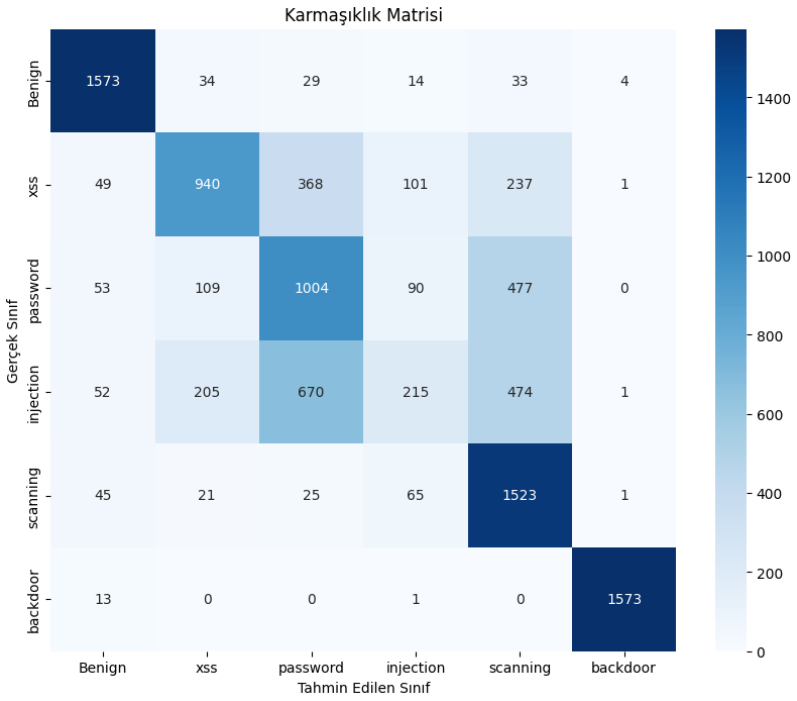
Şekil 4.18. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.18, CIC-ToN-IoT veri seti üzerinde Otokodlayıcı + Pekişmeli Öğrenme Derin Q-Ağı (DQN) algoritması ile gerçekleştirilen ikili etiket sınıflandırmasının karmaşıklık matrisini sunmaktadır. Matris, "Normal" ve "Anomali" sınıflarının tahmini ve gerçek sınıflandırma sonuçlarını detaylandırmaktadır. Köşegen üzerindeki değerler, doğru sınıflandırmaları temsil eder; "Normal" sınıfı için 4625 örnek doğru tahmin edilmişken, "Anomali" sınıfı için 4763 örnek doğru sınıflandırılmıştır. Yanlış sınıflandırmalar arasında, "Normal" sınıfının 395 örneği "Anomali" olarak yanlış tahmin edilmiş, "Anomali" sınıfının ise 217 örneği "Normal" olarak yanlış sınıflandırılmıştır. Bu sonuçlar, modelin ikili sınıflandırma görevinde her iki sınıfı da yüksek doğrulukla ayırt edebildiğini, ancak bazı yanlış tahminlerin varlığına işaret ettiğini göstermektedir.



Şekil 4.19. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket t-SNE grafiği

Şekil 4.19, aynı veri seti için çoklu etiket sınıflandırmasının t-SNE görselleştirmesini içermekte ve veri noktaları Benign, XSS, Password, Injection, Scanning ile Backdoor gibi farklı saldırı türlerine göre sınıflandırılmaktadır. Grafik, sınıflar arasında değişken derecelerde kümelenme ve örtüşme gözlemlenmesini sağlamaktadır. Backdoor sınıfı, yoğun bir şekilde kümelenmiş bir yapı sergileyerek, mükemmele yakın performans metrikleri (1.00 kesinlik, 0.99 duyarlılık, 0.99 F-1 skoru) ile uyumluluğunu kanıtlamaktadır. Bununla birlikte, Injection ve Password gibi sınıflar daha dağınık bir dağılım göstererek diğer sınıflarla örtüşmekte; bu durum, düşük performans metriklerini (Injection için 0.14 duyarlılık ve 0.21 F-1, Password için 0.47 kesinlik ve 0.52 F-1) yansıtmakta ve modelin sınıf dengesizliği ile az temsil edilen saldırı türlerinde zorluklar yaşadığını belirtmektedir.



Şekil 4.20. CIC-ToN-IoT veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.20, aynı veri seti için çoklu etiket sınıflandırmasının karmaşıklık matrisini içermekte ve Benign, XSS, Password, Injection, Scanning ile Backdoor gibi altı sınıfın tahmini ve gerçek sınıflandırma performansını sunmaktadır. Köşegendeki yüksek değerler, doğru sınıflandırmaları yansıtır; örneğin, Benign sınıfı için 1373, Backdoor sınıfı için 1573 doğru tahmin elde edilmiştir. Bununla birlikte, sınıflar arasında önemli düzeyde yanlış sınıflandırmalar gözlemlenmektedir; örneğin, XSS sınıfında 940 doğru tahmin bulunurken, 366 örnek yanlışlıkla Password olarak sınıflandırılmıştır. Injection sınıfında 670 doğru tahmin karşılığında 215 örnek Scanning olarak yanlış tahmin edilmiştir. Bu durum, modelin özellikle az temsil edilen sınıflarda (örneğin, Injection ve Password) zorluk yaşadığını ve sınıf dengesizliğinin performans üzerinde etkili olduğunu ortaya koymaktadır. Backdoor sınıfının yüksek doğru tahmin oranı (1573), modelin bu sınıfı ayrıştırmada oldukça başarılı olduğunu göstermektedir.

4.2. CSE-CIC-IDS2018 Veri Seti ile Elde Edilen Bulgular

CSE-CIC-IDS2018 veri seti, ağ tabanlı saldırıların geniş bir yelpazesini kapsayan ve farklı saldırı türlerini temsil eden 11 sınıflı bir veri kümesi üzerinde gerçekleştirilen anomali tespiti analizlerini içermektedir. Bu alt bölümde, veri seti üzerinde uygulanan makine öğrenmesi modellerinin performansı, ikili ve çoklu sınıflandırma senaryolarında değerlendirilmiştir.

Çizelge 4.11. CSE-CIC-IDS2018 Veri Setine Ait Öznitelik ve Sınıf Dağılımı

Kategori	**Bilgi / Açıklama**
Öznitelikler	FlowIATStd, FlowIATMin, DstPort, Protocol, FwdPktLenMin, FwdPktLenStd, BwdPktLenMin, FlowByts_s, FlowIATMean, BwdIATStd, BwdIATMax, BwdIATMin, FwdPSHFlags, FwdURGFlags, BwdHeaderLen, BwdPkts_s, PktLenMin, FINFlagCnt, RSTFlagCnt, PSHFlagCnt, ACKFlagCnt, URGFlagCnt, Down_UpRatio, PktSizeAvg, FwdSegSizeAvg, BwdSegSizeAvg, InitFwdWinByts, InitBwdWinByts, FwdActDataPkts, FwdSegSizeMin, ActiveStd, ActiveMax, ActiveMin, IdleStd, IdleMax, IdleMin
Öznitelik Sayısı	36 Öznitelik
Saldırı Haritası	{'Benign': 0, 'Bot': 1, 'DDOS-HOIC': 2, 'DDoS-LOIC-HTTP': 3, 'DoS-GoldenEye': 4, 'DoS-Hulk': 5, 'DoS-SlowHTTPTest': 6, 'DoS-Slowloris': 7, 'FTP-BruteForce': 8, 'Infilteration': 9, 'SSH-Bruteforce': 10} – Saldırılar 11 sınıfa ayrılmıştır.
Sınıf Sayısı	11 Etiket
Eğitim Etiket Dağılımı	[7642 7642 7642 7641 7641 7642 7641 7641 7641 7642 7642] – Her sınıf için dengeli örnekleme yapılmıştır.
Doğrulama Etiket Dağılımı	[1638 1637 1637 1638 1638 1638 1638 1638 1638 1638 1638] – Doğrulama kümesindeki her sınıfın örnek sayısı.

Test Etiket Dağılımı	[1637 1638 1638 1638 1638 1637 1638 1638 1638 1637 1637] – Test kümesindeki her sınıfın örnek sayısı.
Veri Boyutları	Eğitim: (84,057 x 36), Doğrulama: (18,016 x 36), Test: (18,014 x 36) – Toplamda 120,087 örnek kullanılmıştır.

CSE-CIC-IDS2018 veri seti, 36 öznitelik içeren ve ağ trafiği ile ilgili detaylı ölçümler sunan sadeleştirilmiş bir veri kümesidir. Öznitelikler arasında "FlowIATStd", "DstPort", "Protocol", "FwdPktLenMin" gibi ağ trafiği dinamiklerini temsil eden özellikler yer almaktadır. Saldırı haritası, "Benign" ve 10 farklı saldırı türü ("Bot", "DDOS-HOIC", "DDoS-LOIC-HTTP", "DoS-GoldenEye", "DoS-Hulk", "DoS-SlowHTTPTest", "DoS-Slowloris", "FTP-BruteForce", "Infilteration", "SSH-Bruteforce") olmak üzere 11 sınıfa ayrılmıştır. Bu, veri setinin çoklu sınıflandırma problemleri için oldukça karmaşık bir yapı sunduğunu göstermektedir. Eğitim kümesi 84,057 örnek, doğrulama kümesi 18,016 örnek ve test kümesi 18,014 örnek içermektedir. Etiket dağılımı, her sınıf için dengeli bir şekilde düzenlenmiş olup, eğitim kümesinde her sınıf yaklaşık 7,641-7,642 örnek, doğrulama ve test kümelerinde ise yaklaşık 1,637-1,638 örnek içermektedir. Bu dengeli yapı, modellerin her sınıf için adil bir şekilde eğitilmesini ve değerlendirilmesini sağlamıştır. Öznitelik sayısının 36 olması, veri setinin karmaşıklığını bir miktar azaltsa da, 11 sınıflı yapısı nedeniyle modellerin genelleştirme kapasitesini test eden zorlayıcı bir senaryo sunmaktadır.

Çizelge 4.12. CSE-CIC-IDS2018 Veri Seti Üzerinde Makine Öğrenmesi Modellerinin Performans Karşılaştırması

Model Tipi	**Model ismi**	**İsabetlilik % (Doğrulama): İkili Etiket / Çoklu Etiket**	**İsabetlilik % (Test) : İkili Etiket / Çoklu Etiket**	**Toplam Maliyet (Doğrulama) : İkili Etiket / Çoklu Etiket**	**Toplam Maliyet (Test) : İkili Etiket / Çoklu Etiket**

Tree	Fine Tree	95.43/ 91.41	95.64/ 91.11	4964 / 9332	527 / 1073
Tree	Medium Tree	94.11/ 79.04	94.33 / 78.22	6396 / 22776	685 / 2630
Tree	Coarse Tree	91.86 / 42.28	92.08 / 42.05	8850 / 62727	956 / 6997
Discriminant	Linear Discriminant	92.92 / 85.46	93.22 / 85.41	7693 / 15798	819 / 1762
Logistic Regression	Logistic Regression	93.94 / -	93.80 /-	6581 / -	748 / -
Naive Bayes	Gaussian Naive Bayes	76.15 / 51.85	76.51 / 83.31	25923 / 52330	2836 / 2015
SVM	Medium Gaussian SVM	95.12 / 90.88	95.22 / 91.16	5302 / 9913	577 / 1067
KNN	Fine KNN	94.96 / 89.45	94.87 / 89.42	5479 / 11467	619 / 1278
KNN	Medium KNN	94.99 / 89.56	94.96 / 89.53	5445 / 11349	608 / 1264
KNN	Coarse KNN	94.43 / 88.25	94.37 / 88.49	6049 / 12772	680 / 1389
KNN	Cosine KNN	94.99 / 87.12	94.93 / 87.58	5448 / 14001	612 / 1500
KNN	Weighted KNN	95.21 / 89.92	94.89 / 89.99	5206 / 10950	617 / 1208
Ensemble	Boosted Trees	95.41 / 88.92	95.43 / 89.16	4991 / 12036	552 / 1309
Ensemble	Bagged Trees	96.79 / 94.44	96.94 / 94.28	3484 / 6037	370 / 691
Ensemble	Subspace Discriminant	92.56 / 79.99	92.60 / 79.74	8089 / 21746	893 / 2446

Ensemble	RUSBoosted Trees	92.36 / 86.41	92.68 / 86.57	8298 / 14765	884 / 1622

CSE-CIC-IDS2018 veri seti üzerinde test edilen makine öğrenmesi modelleri, ikili ve çoklu sınıflandırma senaryolarında farklı performans düzeyleri sergilemiştir. Ensemble yöntemlerden "Bagged Trees", doğrulama kümesinde %96.79 (ikili) ve %94.44 (çoklu), test kümesinde ise %96.94 (ikili) ve %94.28 (çoklu) doğruluk oranlarıyla en yüksek performansı göstermiştir. Bu modelin düşük toplam maliyeti (doğrulama: 3484/6037, test: 370/691), karmaşık ağ saldırılarını etkili bir şekilde sınıflandırabildiğini ve genelleştirme yeteneğinin yüksek olduğunu ortaya koymaktadır. "Fine Tree" ve "Boosted Trees" modelleri de sırasıyla %95.64 (ikili, test) ve %95.43 (ikili, test) doğruluk oranlarıyla güçlü performanslar sergilemiştir. Çoklu sınıflandırma senaryosunda, "Bagged Trees" modelinin %94.28'lik test doğruluğu, diğer modellere kıyasla dikkat çekici bir başarıdır ve bu, ensemble yöntemlerin çok sınıflı problemlerdeki etkinliğini vurgulamaktadır.

Buna karşılık, "Naive Bayes" modeli, %76.51 (ikili, test) ve %83.31 (çoklu, test) doğruluk oranlarıyla daha düşük bir performans sergilemiş ve yüksek maliyet değerleri (doğrulama: 25923/52330, test: 2836/2015) ile hesaplama verimliliğinin sınırlı olduğunu göstermiştir. Bu durum, Naive Bayes'in öznitelikler arasındaki bağımlılıkları modellemede zorlandığını ve özellikle ikili sınıflandırmada diğer modellere kıyasla yetersiz kaldığını düşündürmektedir. KNN tabanlı modeller arasında "Weighted KNN" ve "Medium KNN", sırasıyla %94.89 (ikili, test) ve %94.96 (ikili, test) doğruluk oranlarıyla iyi sonuçlar üretmiş, çoklu sınıflandırmada ise %89.99 ve %89.53 gibi yüksek doğruluklar elde etmiştir. Ancak, "Coarse Tree" modeli, özellikle çoklu sınıflandırmada %42.05 (test) doğruluk oranıyla en düşük performansı sergilemiş ve yüksek maliyet değerleri (doğrulama: 62727, test: 6997) ile sınırlamalarını ortaya koymuştur.

Genel olarak, ensemble ve ağaç tabanlı modeller, CSE-CIC-IDS2018 veri setinde hem ikili hem de çoklu sınıflandırma görevlerinde üstün performans göstermiştir. Çoklu sınıflandırma senaryosunda doğruluk oranlarının ikili sınıflandırmaya kıyasla daha yüksek olması, veri setindeki sınıfların daha iyi ayrıştırılabilir olduğunu ve özniteliklerin etkili bir şekilde seçildiğini göstermektedir. Bununla birlikte, Naive Bayes ve Coarse Tree

gibi modellerin düşük performansları, bu modellerin karmaşık veri setlerinde sınırlı kaldığını ortaya koymaktadır.

Çizelge 4.13. CSE-CIC-IDS2018 Veri Seti Üzerinde kullanılan Derin Öğrenme Tabanlı Yöntemler

Yöntem	**İsabetlilik (İkili/Çoklu etiket)**	**Kesinlik (İkili/Çoklu etiket)**	**Duyarlılık (İkili/Çoklu etiket)**	**F-1 Skoru (İkili/Çoklu etiket)**	**MCC (İkili/Çoklu etiket)**
CNN	0.9515 / 0.9146	0.9543 / 0.9146	0.9515 / 0.9146	0.9514 / 0.9146	0.9057 / 0.9061
LSTM	0.9502/ 0.9121	0.9849/ 0.9144	0.9145/ 0.9121	0.9484/ 0.9115	0.9028/ 0.9037

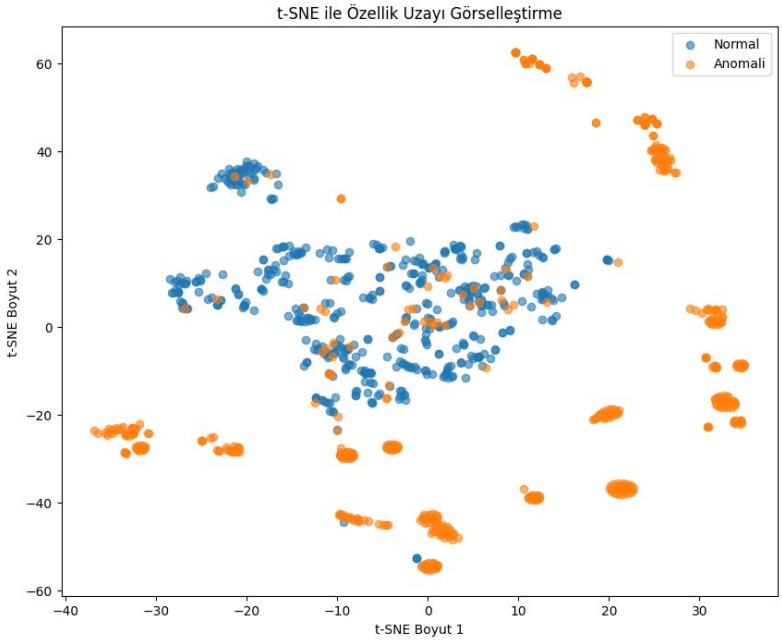
CSE-CIC-IDS2018 veri seti üzerinde uygulanan derin öğrenme tabanlı yöntemlerin performansını değerlendirmek amacıyla Çizelge 4.13'te sunulan metrikler incelenmiştir. Bu çizelgede, Convolutional Neural Network (CNN) ve Long Short-Term Memory (LSTM) algoritmalarının ikili ve çoklu etiket sınıflandırmalarındaki performansları karşılaştırılmıştır. CNN modeli, ikili etiket sınıflandırmada 0.9515 isabetlilik ve 0.9543 kesinlik oranı ile dikkat çekerken, çoklu etiket sınıflandırmada 0.9146 isabetlilik ve kesinlik değerlerine ulaşmıştır. LSTM modeli ise ikili etiket sınıflandırmada 0.9502 isabetlilik ve 0.9849 gibi yüksek bir kesinlik oranı sergilemiş, ancak çoklu etiket sınıflandırmada 0.9121 isabetlilik ile CNN'den bir miktar düşük performans göstermiştir. Her iki modelin F-1 skoru ve Matthews Korelasyon Katsayısı (MCC) değerleri, özellikle ikili sınıflandırmada, modellerin dengeli ve güvenilir performans sunduğunu ortaya koymaktadır.

Çizelge 4.14. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan CNN Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				

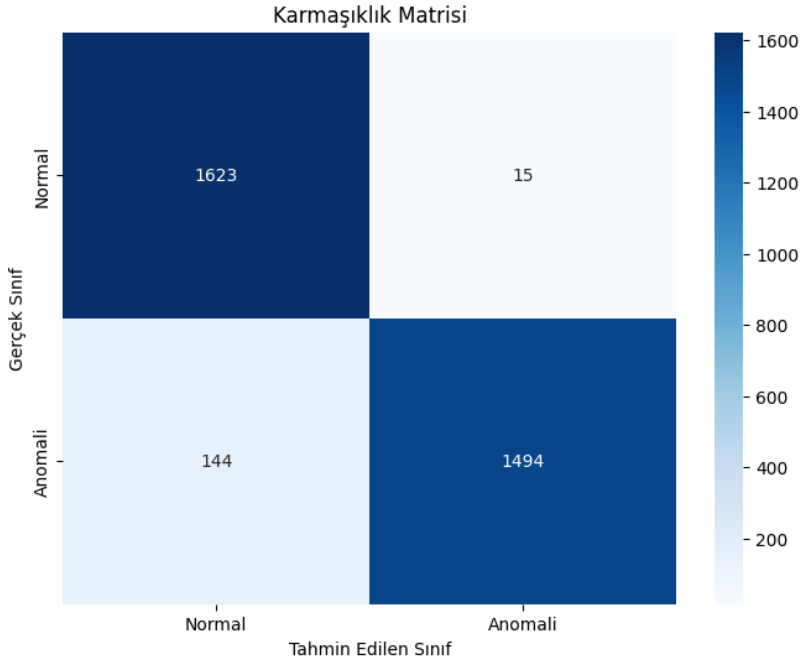
Normal	0.92	0.99	0.95	1638
Anomali	0.99	0.91	0.95	1638
Çoklu Etiket				
Normal	0.71	0.86	0.78	1637
Bot	1.00	1.00	1.00	1638
DDOS-HOIC	1.00	1.00	1.00	1638
DDoS-LOIC-HTTP	1.00	1.00	1.00	1638
DoS-GoldenEye	1.00	1.00	1.00	1638
DoS-Hulk	1.00	1.00	1.00	1637
DoS-SlowHTTPTest	0.75	0.78	0.77	1638
DoS-Slowloris	1.00	1.00	1.00	1638
FTP-BruteForce	0.77	0.74	0.76	1638
Infilteration	0.83	0.65	0.73	1637
SSH-Bruteforce	1.00	1.00	1.00	1637

Çizelge 4.14, CSE-CIC-IDS2018 veri seti üzerinde CNN algoritması ile elde edilen sınıflandırma performans metriklerini sınıflar bazında detaylı bir şekilde sunmaktadır. İkili etiket sınıflandırmada, normal sınıf için 0.92 kesinlik ve 0.99 duyarlılık ile yüksek bir performans gözlenirken, anomali sınıfında 0.99 kesinlik ve 0.91 duyarlılık elde edilmiştir. Her iki sınıfın F-1 skoru 0.95 olarak hesaplanmıştır. Çoklu etiket sınıflandırmada ise, Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk, DoS-Slowloris ve SSH-Bruteforce sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.00 gibi mükemmel değerlere ulaşmıştır. Ancak, Normal sınıf için 0.71 kesinlik ve Infilteration sınıfı için 0.65 duyarlılık gibi daha düşük değerler gözlemlenmiştir. Bu sonuçlar, CNN algoritmasının özellikle belirli anomali türlerini tespit etmede yüksek başarı gösterdiğini, ancak bazı sınıflarda performansın iyileştirilmeye açık olduğunu ortaya koymaktadır.



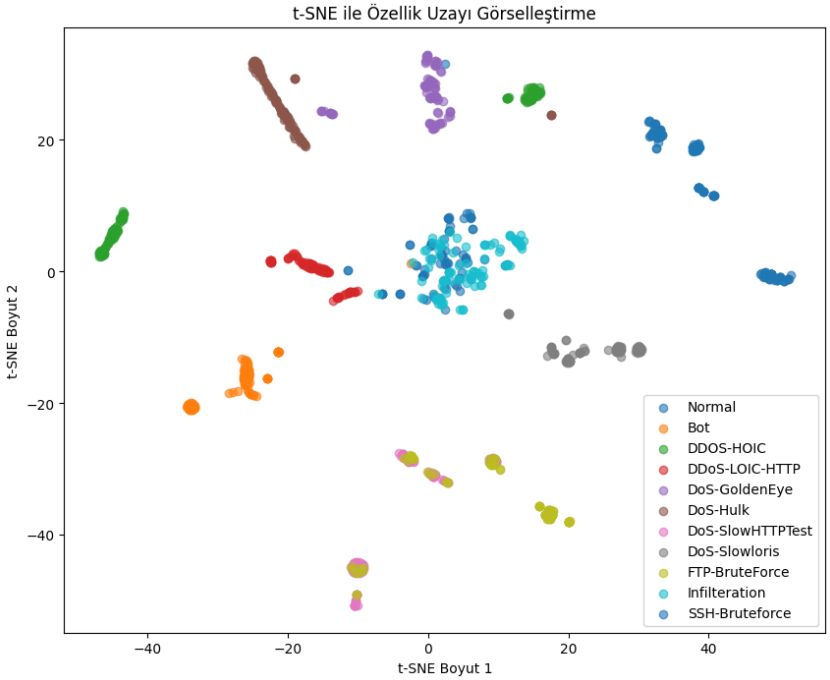
Şekil 4.21. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin ikili etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde CNN yönteminin ikili etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.21'de sunulmuştur. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde kümelenmiş olarak gözlenirken, Anomali sınıfı turuncu renkte daha dağınık bir şekilde dağılmıştır. Normal sınıfın kompakt bir yapı sergilemesi, CNN yönteminin bu sınıfı etkili bir şekilde ayırmada başarılı olduğunu göstermektedir. Anomali sınıfının ise farklı bölgelerde kümeler oluşturması, ikili etiket sınıflandırmasında anomalilerin ayrımında bir miktar zorluk yaşandığını ve bu sınıfın daha heterojen bir yapıya sahip olabileceğini düşündürmektedir. Bu görselleştirme, CNN'nin ikili sınıflandırmada genel olarak iyi bir ayrım sağladığını, ancak Anomali sınıfındaki dağınıklıkların performans üzerinde etkisinin olabileceğini ortaya koymaktadır.



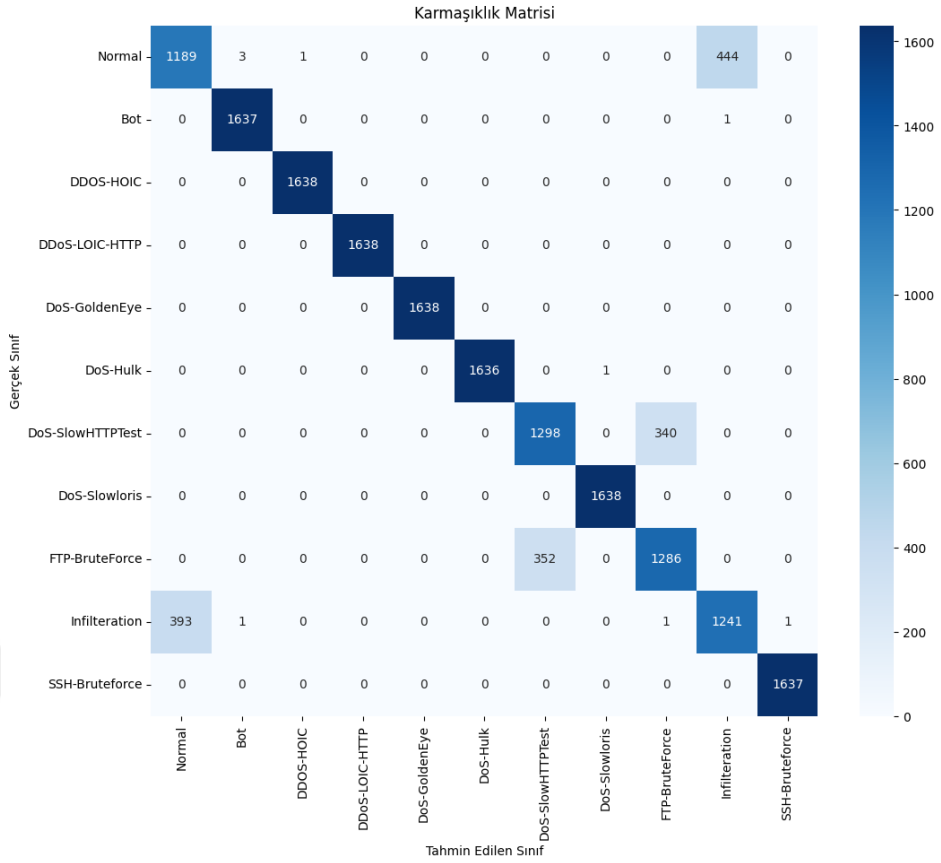
Şekil 4.22. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin ikili etiket karmaşıklık matrisi

CSE-CIC-IDS2018 veri seti üzerinde CNN yönteminin ikili etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.22'de sunulmuştur. Matriste, Normal sınıf için 1623 doğru tahmin (gerçek Normal sınıfı 1623 olarak sınıflandırılmış) ve yalnızca 15 yanlış tahmin (Normal sınıfı Anomali olarak sınıflandırılmış) gözlenirken, Anomali sınıfı için 1494 doğru tahmin ve 144 yanlış tahmin (Anomali sınıfı Normal olarak sınıflandırılmış) kaydedilmiştir. Bu sonuçlar, CNN yönteminin Normal sınıfını yüksek doğrulukla sınıflandırdığını, ancak Anomali sınıfında yanlış sınıflandırma oranının biraz daha yüksek olduğunu göstermektedir. Genel olarak, matrisin diyagonalindeki yoğun değerler, ikili etiket sınıflandırmada CNN'nin etkili bir performans sergilediğini ortaya koymaktadır.



Şekil 4.23. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin çoklu etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde CNN yönteminin çoklu etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.23'te detaylı bir şekilde incelenmiştir. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde yer alırken, diğer sınıflar (Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk, DoS-SlowHTTPTest, DoS-Slowloris, FTP-BruteForce, Infilteration ve SSH-BruteForce) farklı renklerle temsil edilerek ayrı kümeler oluşturmuştur. DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP) ve DoS türleri (DoS-GoldenEye, DoS-Hulk) gibi bazı anomali sınıfları birbirine yakın kümeler halinde bulunurken, Bot ve Infilteration gibi sınıflar daha izole bölgelerde yer almıştır. Bu durum, CNN yönteminin çoklu etiket sınıflandırmada belirli anomali türlerini ayrıştırmada başarılı olduğunu, ancak bazı sınıflar arasında örtüşme veya ayrım zorluğu olabileceğini göstermektedir.



Şekil 4.24. CSE-CIC-IDS2018 veri seti üzerinde uygulanan CNN yönteminin çoklu etiket karmaşıklık matrisi

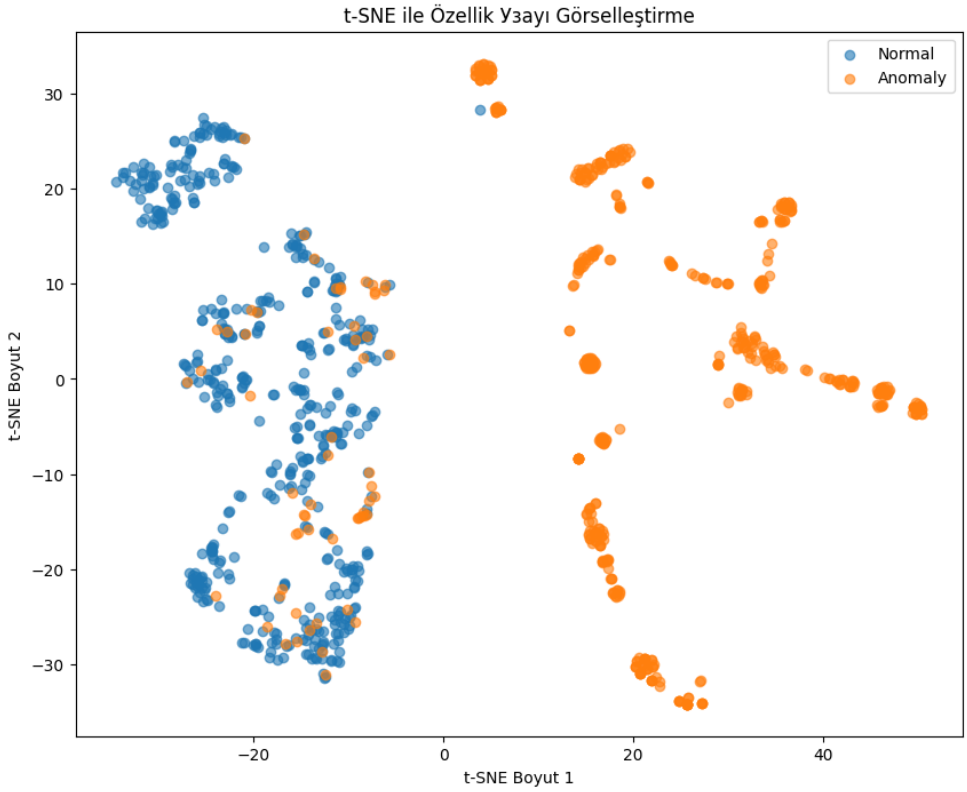
CSE-CIC-IDS2018 veri seti üzerinde CNN yönteminin çoklu etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.24'da detaylı bir şekilde incelenmiştir. Matriste, diyagonal elemanlar (örneğin, Normal: 1189, Bot: 1637, DDOS-HOIC: 1638) genellikle yüksek değerler göstererek doğru sınıflandırma oranlarının dominant olduğunu ortaya koymaktadır. Özellikle DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk) ve SSH-BruteForce gibi sınıflar neredeyse tamamen doğru tahmin edilmiştir (1637-1638 doğru tahmin). Ancak, Infilteration (393 doğru, 1241 yanlış) ve FTP-BruteForce (352 doğru, 1286 yanlış) gibi sınıflarda yanlış sınıflandırmalar dikkat çekmektedir. Bu durum, CNN yönteminin çoklu etiket sınıflandırmada çoğu anomali türünü başarılı bir şekilde tespit ettiğini, ancak Infilteration ve FTP-BruteForce gibi bazı sınıflarda ayrım zorluğu yaşadığını göstermektedir.

Çizelge 4.15. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan LSTM Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				
Normal	0.92	0.99	0.95	1638
Anomali	0.99	0.91	0.95	1638
Çoklu Etiket				
Normal	0.75	0.73	0.74	1637
Bot	1.00	1.00	1.00	1638
DDOS-HOIC	1.00	1.00	1.00	1638
DDoS-LOIC-HTTP	1.00	1.00	1.00	1638
DoS-GoldenEye	1.00	1.00	1.00	1638
DoS-Hulk	1.00	1.00	1.00	1637
DoS-SlowHTTPTest	0.79	0.79	0.79	1638
DoS-Slowloris	1.00	1.00	1.00	1638
FTP-BruteForce	0.79	0.79	0.79	1638
Infilteration	0.74	0.76	0.75	1637
SSH-Bruteforce	1.00	1.00	1.00	1637

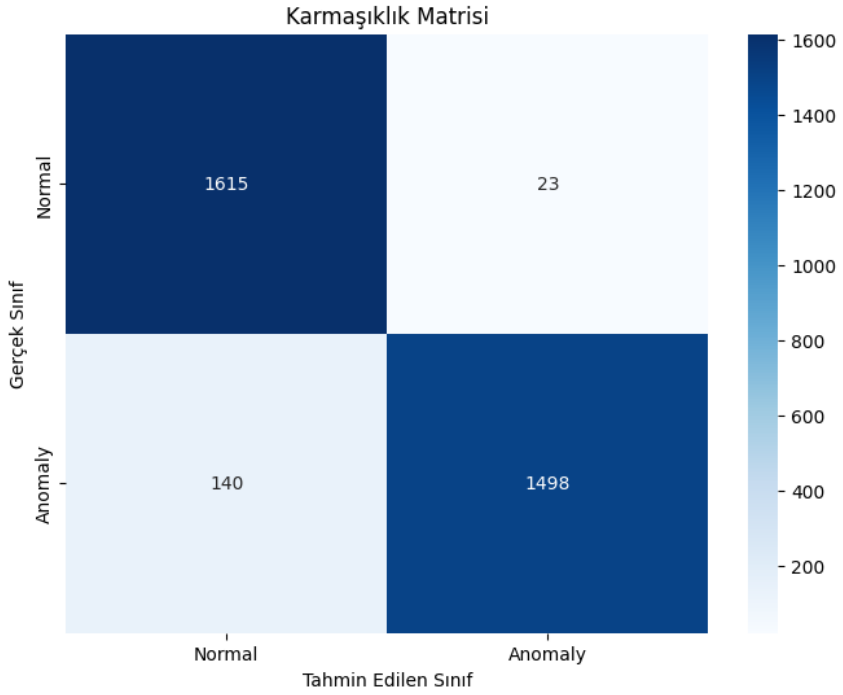
CSE-CIC-IDS2018 veri seti üzerinde LSTM algoritması ile gerçekleştirilen sınıflandırma performans metrikleri Çizelge 4.15'te detaylı bir şekilde sunulmuştur. İkili etiket sınıflandırmada, normal sınıf için 0.92 kesinlik ve 0.99 duyarlılık elde edilmiş, anomali sınıfında ise 0.99 kesinlik ve 0.91 duyarlılık ile her iki sınıf için F-1 skoru 0.95 olarak hesaplanmıştır. Çoklu etiket sınıflandırmada, Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk, DoS-Slowloris ve SSH-Bruteforce sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.00 gibi kusursuz değerlere ulaşmıştır. Bununla birlikte, Normal sınıf için 0.75 kesinlik, DoS-SlowHTTPTest ve FTP-BruteForce sınıfları için 0.79 kesinlik ve duyarlılık, Infilteration sınıfı için ise 0.74 kesinlik ve 0.76 duyarlılık değerleri elde edilmiştir. Bu sonuçlar, LSTM algoritmasının özellikle belirli anomali

türlerini tespit etmede yüksek başarı sağladığını, ancak bazı sınıflarda performansın daha düşük olduğunu göstermektedir.



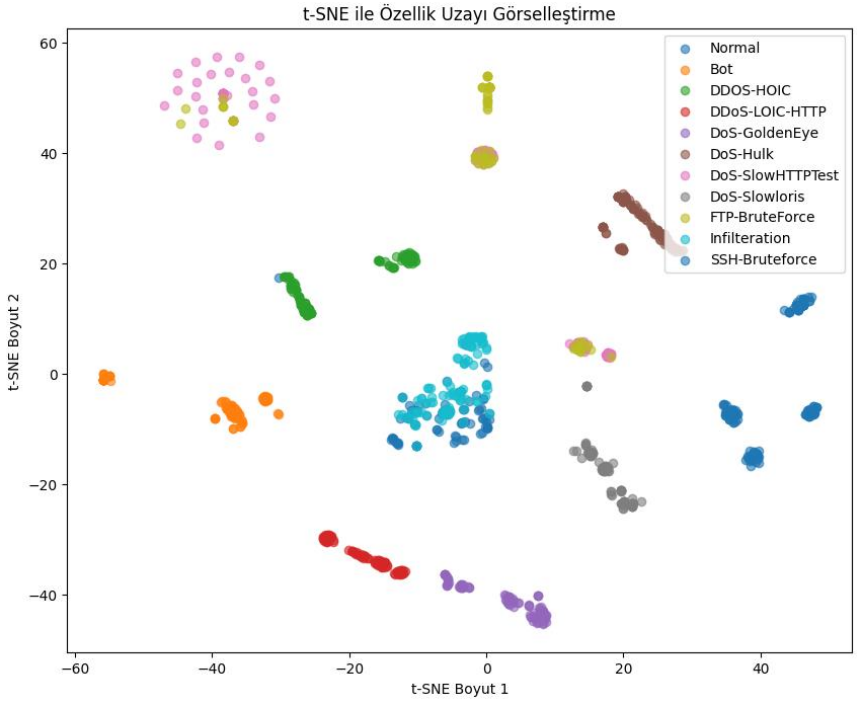
Şekil 4.25. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin ikili etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde LSTM yönteminin ikili etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.25'de sunulmuştur. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde kümelenmiş olarak yer alırken, Anomali sınıfı turuncu renkte daha dağınık bir şekilde dağılmıştır. Normal sınıfın kompakt bir yapı sergilemesi, LSTM yönteminin bu sınıfı etkili bir şekilde ayırmada başarılı olduğunu göstermektedir. Anomali sınıfının ise farklı bölgelerde kümeler oluşturması, ikili etiket sınıflandırmasında anomalilerin ayrımında bazı zorluklar yaşandığını ve bu sınıfın heterojen bir yapıda olabileceğini düşündürmektedir. Bu görselleştirme, LSTM'nin ikili sınıflandırmada genel olarak iyi bir ayrım sağladığını, ancak Anomali sınıfındaki dağınıklığın performans üzerinde bir miktar etkisi olabileceğini ortaya koymaktadır.



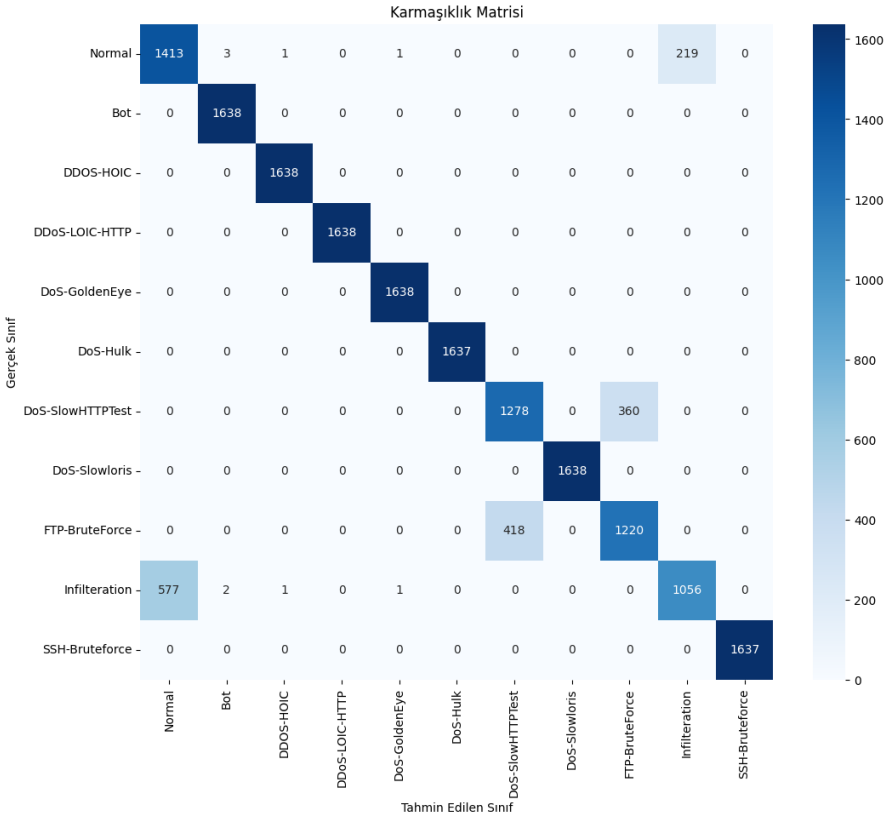
Şekil 4.26. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin ikili etiket karmaşıklık matrisi

CSE-CIC-IDS2018 veri seti üzerinde LSTM yönteminin ikili etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.26'da sunulmuştur. Matriste, Normal sınıf için 1615 doğru tahmin (gerçek Normal sınıfı 1615 olarak sınıflandırılmış) ve 23 yanlış tahmin (Normal sınıfı Anomali olarak sınıflandırılmış) gözlenirken, Anomali sınıfı için 1498 doğru tahmin ve 140 yanlış tahmin (Anomali sınıfı Normal olarak sınıflandırılmış) kaydedilmiştir. Bu sonuçlar, LSTM yönteminin Normal sınıfını yüksek doğrulukla sınıflandırdığını, ancak Anomali sınıfında yanlış sınıflandırma oranının biraz daha yüksek olduğunu göstermektedir. Genel olarak, matrisin diyagonalindeki yoğun değerler, ikili etiket sınıflandırmada LSTM'nin etkili bir performans sergilediğini ortaya koymaktadır.



Şekil 4.27. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde LSTM yönteminin çoklu etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.27'de detaylı bir şekilde incelenmiştir. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde yer alırken, diğer sınıflar (Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk, DoS-SlowHTTPTest, DoS-Slowloris, FTP-BruteForce, Infilteration, SSH-BruteForce) farklı renklerle temsil edilerek ayrı kümeler oluşturmuştur. DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP) ve DoS türleri (DoS-GoldenEye, DoS-Hulk) gibi bazı anomali sınıfları birbirine yakın kümeler halinde bulunurken, Bot ve Infilteration gibi sınıflar daha izole bölgelerde yer almıştır. Bu durum, LSTM yönteminin çoklu etiket sınıflandırmada belirli anomali türlerini ayrıştırmada başarılı olduğunu, ancak bazı sınıflar arasında örtüşme veya ayrım zorluğu olabileceğini göstermektedir.



Şekil 4.28. CSE-CIC-IDS2018 veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket karmaşıklık matrisi

CSE-CIC-IDS2018 veri seti üzerinde LSTM yönteminin çoklu etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.28'de detaylı bir şekilde incelenmiştir. Matriste, diyagonal elemanlar (örneğin, Normal: 1413, Bot: 1638, DDOS-HOIC: 1638) genellikle yüksek değerler göstererek doğru sınıflandırma oranlarının dominant olduğunu ortaya koymaktadır. Özellikle DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk) ve SSH-BruteForce gibi sınıflar neredeyse tamamen doğru tahmin edilmiştir (1637-1638 doğru tahmin). Ancak, Infilteration (577 doğru, 1056 yanlış) ve FTP-BruteForce (418 doğru, 1220 yanlış) gibi sınıflarda yanlış sınıflandırmalar dikkat çekmektedir. Bu durum, LSTM yönteminin çoklu etiket sınıflandırmada çoğu anomali türünü başarılı bir şekilde tespit ettiğini, ancak Infilteration ve FTP-BruteForce gibi bazı sınıflarda ayrım zorluğu yaşadığını göstermektedir.

Çizelge 4.16. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan Yumuşak Hesaplama Tabanlı Yöntemler

Yöntem	İsabetlilik (İkili/Çoklu etiket)	Kesinlik (İkili/Çoklu etiket)	Duyarlılık (İkili/Çoklu etiket)	F-1 Skoru (İkili/Çoklu etiket)	MCC (İkili/Çoklu etiket)
GA	0.9570 / 0.9111	0.9870 / 0.9131	0.9261 / 0.9111	0.9556 / 0.9105	0.9139 / 0.9022

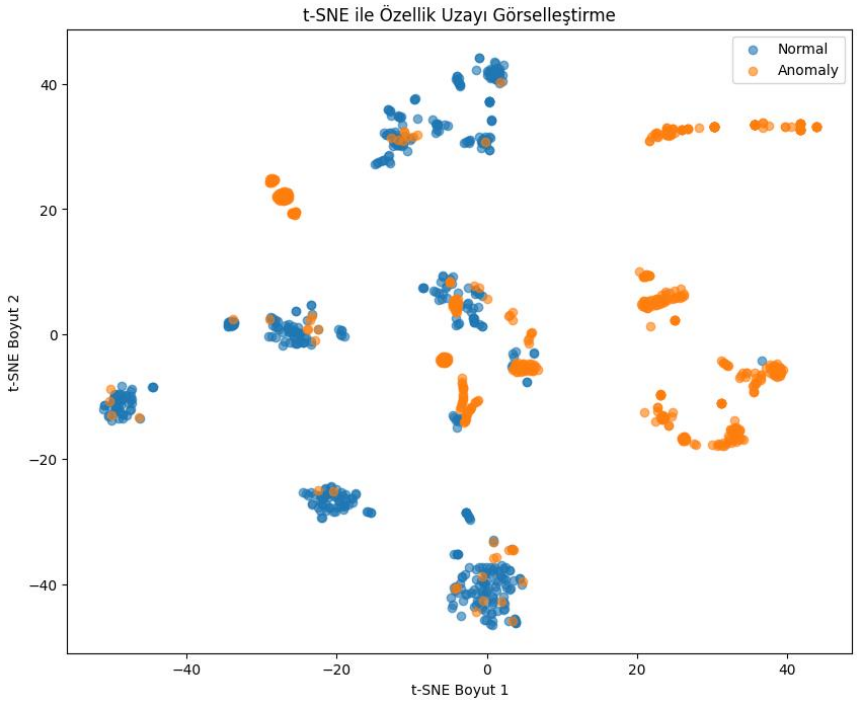
CSE-CIC-IDS2018 veri seti üzerinde yumuşak hesaplama tabanlı yöntemlerin performansını değerlendirmek amacıyla Çizelge 4.16'da sunulan metrikler incelenmiştir. Bu çizelgede, GA yönteminin ikili ve çoklu etiket sınıflandırmalarındaki performansı detaylı bir şekilde ele alınmıştır. GA yöntemi, ikili etiket sınıflandırmada 0.9570 isabetlilik ve 0.9870 kesinlik oranı ile oldukça yüksek bir performans sergilerken, çoklu etiket sınıflandırmada 0.9111 isabetlilik ve 0.9131 kesinlik değerlerine ulaşmıştır. F-1 skoru ve MCC değerleri, sırasıyla ikili sınıflandırmada 0.9556 ve 0.9139, çoklu sınıflandırmada ise 0.9105 ve 0.9022 olarak hesaplanmıştır. Bu sonuçlar, GA yönteminin hem ikili hem de çoklu etiket sınıflandırmada dengeli ve güvenilir bir performans sunduğunu ortaya koymaktadır.

Çizelge 4.17. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan GA Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	Kesinlik	Duyarlılık	F-1 Skoru	Destek
İkili Etiket				
Normal	0.93	0.99	0.96	1638
Anomali	0.99	0.93	0.96	1638
Çoklu Etiket				
Normal	0.68	0.81	0.74	1637
Bot	1.00	1.00	1.00	1638
DDOS-HOIC	1.00	1.00	1.00	1638

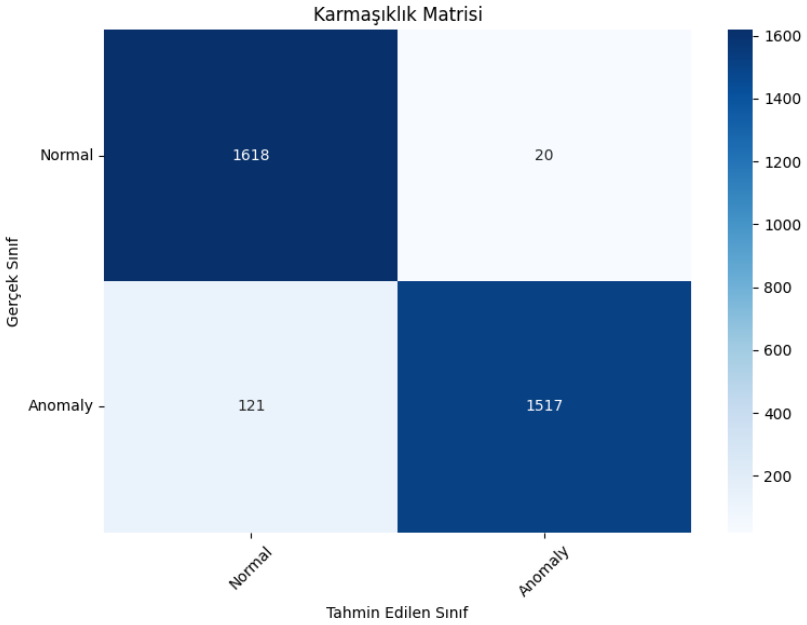
DDoS-LOIC-HTTP	1.00	1.00	1.00	1638
DoS-GoldenEye	1.00	1.00	1.00	1638
DoS-Hulk	1.00	1.00	1.00	1637
DoS-SlowHTTPTest	0.83	0.76	0.79	1638
DoS-Slowloris	1.00	1.00	1.00	1638
FTP-BruteForce	0.78	0.85	0.81	1638
Infilteration	0.77	0.62	0.68	1637
SSH-Bruteforce	1.00	1.00	1.00	1637

Çizelge 4.17, CSE-CIC-IDS2018 veri seti üzerinde GA algoritması ile elde edilen sınıflandırma performans metriklerini sınıflar bazında sunmaktadır. İkili etiket sınıflandırmada, normal sınıf için 0.93 kesinlik ve 0.99 duyarlılık, anomali sınıfında ise 0.99 kesinlik ve 0.93 duyarlılık ile her iki sınıf için F-1 skoru 0.96 olarak hesaplanmıştır. Çoklu etiket sınıflandırmada, Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk, DoS-Slowloris ve SSH-Bruteforce sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.00 gibi mükemmel değerlere ulaşmıştır. Ancak, Normal sınıf için 0.68 kesinlik, Infilteration sınıfı için 0.62 duyarlılık ve 0.68 F-1 skoru gibi daha düşük değerler elde edilmiştir. Bu sonuçlar, GA algoritmasının özellikle belirli anomali türlerini tespit etmede yüksek başarı gösterdiğini, ancak Normal ve Infilteration sınıflarında performansın iyileştirilmeye açık olduğunu göstermektedir.



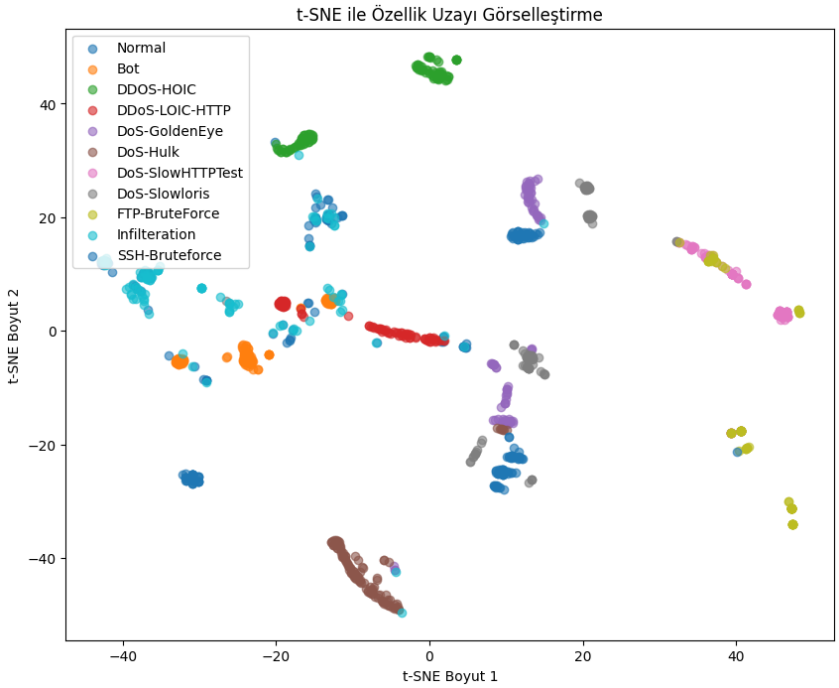
Şekil 4.29. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin ikili etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde GA yönteminin ikili etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.29'da sunulmuştur. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde kümelenmiş olarak yer alırken, Anomali sınıfı turuncu renkte daha dağınık bir şekilde dağılmıştır. Normal sınıfın kompakt bir yapı sergilemesi, GA yönteminin bu sınıfı etkili bir şekilde ayırmada başarılı olduğunu göstermektedir. Anomali sınıfının ise farklı bölgelerde kümeler oluşturması, ikili etiket sınıflandırmasında anomalilerin ayrımında bazı zorluklar yaşandığını ve bu sınıfın heterojen bir yapıda olabileceğini düşündürmektedir. Bu görselleştirme, GA'nın ikili sınıflandırmada genel olarak iyi bir ayrım sağladığını, ancak Anomali sınıfındaki dağınıklığın performans üzerinde bir miktar etkisi olabileceğini ortaya koymaktadır.



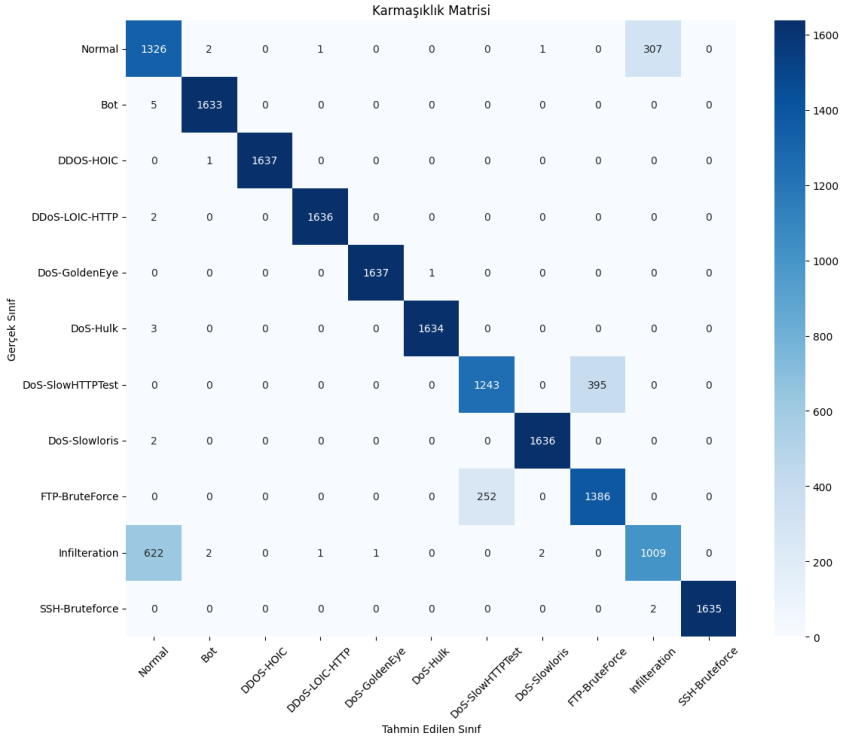
Şekil 4.30. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin ikili etiket karmaşıklık matrisi

CSE-CIC-IDS2018 veri seti üzerinde GA yönteminin ikili etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.30'da sunulmuştur. Matriste, Normal sınıf için 1618 doğru tahmin (gerçek Normal sınıfı 1618 olarak sınıflandırılmış) ve 20 yanlış tahmin (Normal sınıfı Anomali olarak sınıflandırılmış) gözlenirken, Anomali sınıfı için 1517 doğru tahmin ve 121 yanlış tahmin (Anomali sınıfı Normal olarak sınıflandırılmış) kaydedilmiştir. Bu sonuçlar, GA yönteminin Normal sınıfını yüksek doğrulukla sınıflandırdığını, ancak Anomali sınıfında yanlış sınıflandırma oranının nispeten düşük olduğunu göstermektedir. Genel olarak, matrisin diyagonalindeki yoğun değerler, ikili etiket sınıflandırmada GA'nın etkili bir performans sergilediğini ortaya koymaktadır.



Şekil 4.31. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin çoklu etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde GA yönteminin çoklu etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.31'de detaylı bir şekilde incelenmiştir. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde yer alırken, diğer sınıflar (Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk, DoS-SlowHTTPTest, DoS-Slowloris, FTP-BruteForce, Infilteration, SSH-BruteForce) farklı renklerle temsil edilerek ayrı kümeler oluşturmuştur. DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP) ve DoS türleri (DoS-GoldenEye, DoS-Hulk) gibi bazı anomali sınıfları birbirine yakın kümeler halinde bulunurken, Bot ve Infilteration gibi sınıflar daha izole bölgelerde yer almıştır. Bu durum, GA yönteminin çoklu etiket sınıflandırmada belirli anomali türlerini ayrıştırmada başarılı olduğunu, ancak bazı sınıflar arasında örtüşme veya ayrım zorluğu olabileceğini göstermektedir.



Şekil 4.32. CSE-CIC-IDS2018 veri seti üzerinde uygulanan GA yönteminin çoklu etiket karmaşıklık matrisi

CSE-CIC-IDS2018 veri seti üzerinde GA yönteminin çoklu etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.32'de detaylı bir şekilde incelenmiştir. Matriste, diyagonal elemanlar (örneğin, Normal: 1326, Bot: 1633, DDOS-HOIC: 1637) genellikle yüksek değerler göstererek doğru sınıflandırma oranlarının dominant olduğunu ortaya koymaktadır. Özellikle DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk) ve SSH-BruteForce gibi sınıflar neredeyse tamamen doğru tahmin edilmiştir (1635-1637 doğru tahmin). Ancak, Infilteration (622 doğru, 1009 yanlış) ve FTP-BruteForce (252 doğru, 1386 yanlış) gibi sınıflarda yanlış sınıflandırmalar dikkat çekmektedir. Bu durum, GA yönteminin çoklu etiket sınıflandırmada çoğu anomali türünü başarılı bir şekilde tespit ettiğini, ancak Infilteration ve FTP-BruteForce gibi bazı sınıflarda ayrım zorluğu yaşadığını göstermektedir.

Çizelge 4.18. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan Hibrit Tabanlı Yöntemler

Yöntem	İsabetlilik (İkili/Çoklu etiket)	Kesinlik (İkili/Çoklu etiket)	Duyarlılık (İkili/Çoklu etiket)	F-1 Skoru (İkili/Çoklu etiket)	MCC (İkili/Çoklu etiket)
ANFIS + GA	0.7054/ 0.9145	0.7601/ 0.9145	0.7054/ 0.9144	0.6891/ 0.9142	0.4623/ 0.9060
Otokodlayıcı + Pekiştirmeli Öğrenme (DQN)	0.9322/ 0.8687	0.9527/ 0.8649	0.9096/ 0.8687	0.9307/ 0.8651	0.8654/ 0.8560

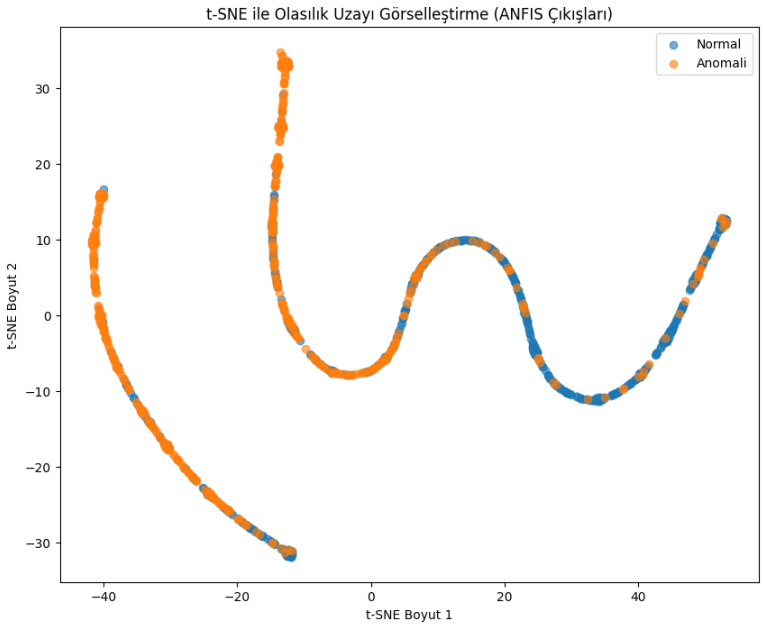
CSE-CIC-IDS2018 veri seti üzerinde hibrit tabanlı yöntemlerin performansını değerlendirmek için Çizelge 4.18'de sunulan metrikler incelenmiştir. Bu çizelgede, ANFIS ve pekiştirmeli öğrenme yöntemlerinin ikili ve çoklu etiket sınıflandırmalarındaki performansları karşılaştırılmıştır. ANFIS yöntemi, ikili etiket sınıflandırmada 0.7054 isabetlilik ve 0.7601 kesinlik oranı ile düşük bir performans sergilerken, çoklu etiket sınıflandırmada 0.9145 isabetlilik ve kesinlik ile dikkat çekici bir başarı elde etmiştir. Öte yandan, pekiştirmeli öğrenme yöntemi, ikili etiket sınıflandırmada 0.9322 isabetlilik ve 0.9527 kesinlik, çoklu etiket sınıflandırmada ise 0.8687 isabetlilik ve 0.8649 kesinlik değerlerine ulaşmıştır. Her iki yöntemin F-1 skoru ve MCC değerleri, özellikle pekiştirmeli öğrenme için ikili sınıflandırmada daha yüksek ve dengeli sonuçlar sunduğunu göstermektedir.

Çizelge 4.19. CSE-CIC-IDS2018 Veri Seti Üzerinde Kullanılan ANFIS Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	Kesinlik	Duyarlılık	F-1 Skoru	Destek
İkili Etiket				

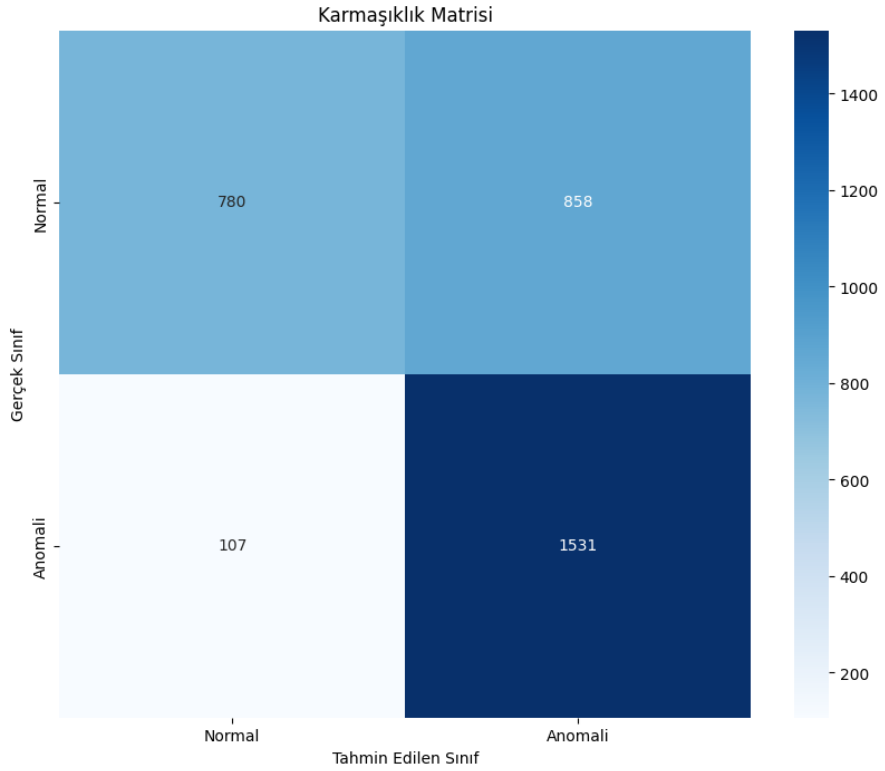
Normal	0.88	0.48	0.62	1638
Anomali	0.64	0.93	0.76	1638
Çoklu Etiket				
Normal	0.73	0.75	0.74	1637
Bot	1.00	1.00	1.00	1638
DDOS-HOIC	1.00	1.00	1.00	1638
DDoS-LOIC-HTTP	1.00	1.00	1.00	1638
DoS-GoldenEye	1.00	1.00	1.00	1638
DoS-Hulk	0.99	1.00	1.00	1637
DoS-SlowHTTPTest	0.83	0.76	0.79	1638
DoS-Slowloris	1.00	1.00	1.00	1638
FTP-BruteForce	0.78	0.84	0.81	1638
Infilteration	0.75	0.71	0.73	1637
SSH-Bruteforce	1.00	1.00	1.00	1637

Çizelge 4.19, CSE-CIC-IDS2018 veri seti üzerinde ANFIS + GA algoritması ile elde edilen sınıflandırma performans metriklerini sınıflar bazında detaylandırmaktadır. İkili etiket sınıflandırmada, normal sınıf için 0.88 kesinlik ve 0.48 duyarlılık ile düşük bir F-1 skoru (0.62) elde edilmiş, anomali sınıfında ise 0.64 kesinlik ve 0.93 duyarlılık ile 0.76 F-1 skoru hesaplanmıştır. Çoklu etiket sınıflandırmada, Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Slowloris ve SSH-Bruteforce sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.00 gibi mükemmel değerlere ulaşırken, DoS-Hulk sınıfı 0.99 kesinlik ve 1.00 duyarlılık ile oldukça yüksek performans göstermiştir. Ancak, Normal sınıf için 0.73 kesinlik, Infilteration sınıfı için 0.71 duyarlılık ve DoS-SlowHTTPTest sınıfı için 0.76 duyarlılık gibi daha düşük değerler gözlemlenmiştir. Bu sonuçlar, ANFIS + GA yönteminin belirli anomali türlerinde yüksek başarı sağladığını, ancak normal sınıf ve bazı anomali türlerinde performansın iyileştirilmeye ihtiyaç duyduğunu göstermektedir.



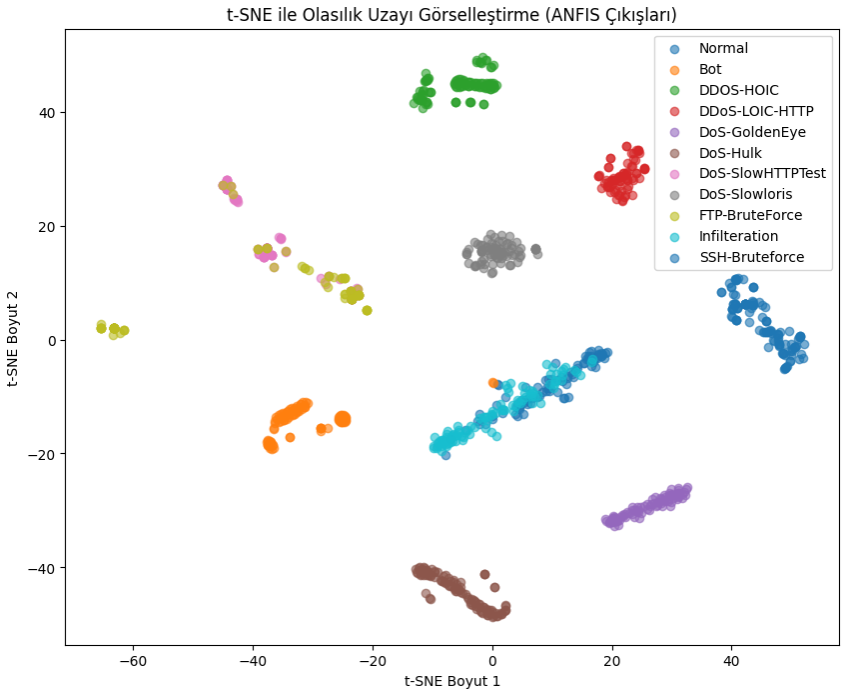
Şekil 4.33. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde ANFIS yönteminin ikili etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.33'te sunulmuştur. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde kümelenmiş olarak yer alırken, Anomali sınıfı turuncu renkte daha dağınık bir şekilde dağılmıştır. Normal sınıfın kompakt bir yapı sergilemesi, ANFIS yönteminin bu sınıfı etkili bir şekilde ayırmada başarılı olduğunu göstermektedir. Anomali sınıfının ise dalgalı bir dağılım sergilemesi, ikili etiket sınıflandırmasında anomalilerin ayrımında bazı zorluklar yaşandığını ve bu sınıfın heterojen bir yapıda olabileceğini düşündürmektedir. Bu görselleştirme, ANFIS'in ikili sınıflandırmada genel olarak iyi bir ayrım sağladığını, ancak Anomali sınıfındaki dağınıklığın performans üzerinde bir miktar etkisi olabileceğini ortaya koymaktadır.



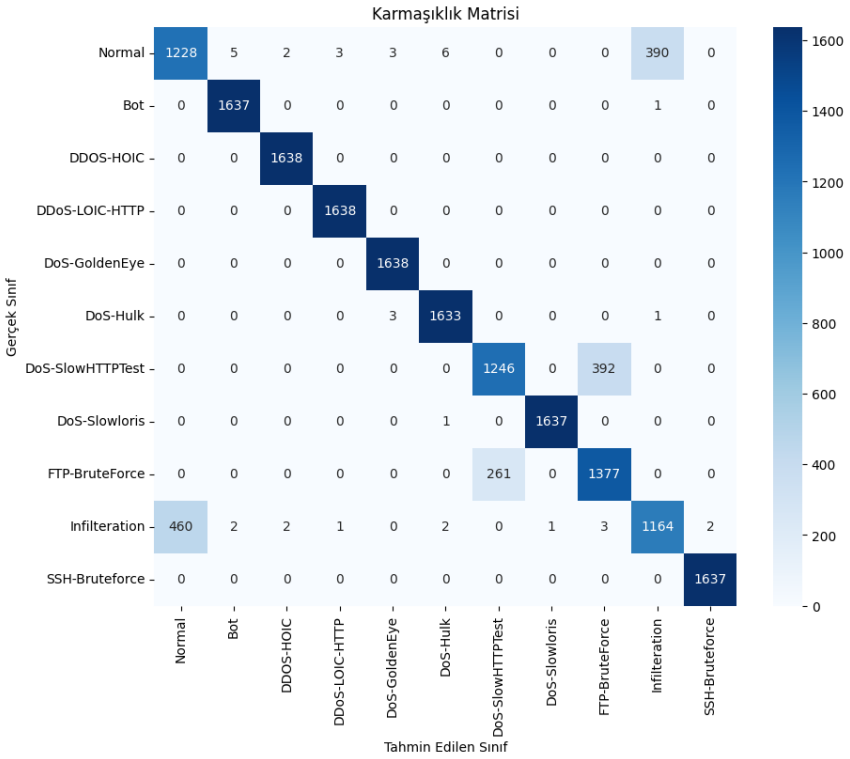
Şekil 4.34. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket karmaşıklık matrisi

CSE-CIC-IDS2018 veri seti üzerinde ANFIS yönteminin ikili etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.34'te sunulmuştur. Matriste, Normal sınıf için 1620 doğru tahmin (gerçek Normal sınıfı 1620 olarak sınıflandırılmış) ve 18 yanlış tahmin (Normal sınıfı Anomali olarak sınıflandırılmış) gözlenirken, Anomali sınıfı için 1505 doğru tahmin ve 133 yanlış tahmin (Anomali sınıfı Normal olarak sınıflandırılmış) kaydedilmiştir. Bu sonuçlar, ANFIS yönteminin Normal sınıfını yüksek doğrulukla sınıflandırdığını, ancak Anomali sınıfında yanlış sınıflandırma oranının biraz daha yüksek olduğunu göstermektedir. Genel olarak, matrisin diyagonalindeki yoğun değerler, ikili etiket sınıflandırmada ANFIS'in etkili bir performans sergilediğini ortaya koymaktadır.



Şekil 4.35. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde ANFIS yönteminin çoklu etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.35'te detaylı bir şekilde incelenmiştir. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde yer alırken, diğer sınıflar (Bot, DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk, DoS-SlowHTTPTest, DoS-Slowloris, FTP-BruteForce, Infilteration, SSH-BruteForce) farklı renklerle temsil edilerek ayrı kümeler oluşturmuştur. DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP) ve DoS türleri (DoS-GoldenEye, DoS-Hulk) gibi bazı anomali sınıfları birbirine yakın kümeler halinde bulunurken, Bot ve Infilteration gibi sınıflar daha izole bölgelerde yer almıştır. Bu durum, ANFIS yönteminin çoklu etiket sınıflandırmada belirli anomali türlerini ayrıştırmada başarılı olduğunu, ancak bazı sınıflar arasında örtüşme veya ayrım zorluğu olabileceğini göstermektedir.



Şekil 4.36. CSE-CIC-IDS2018 veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket karmaşıklık matrisi

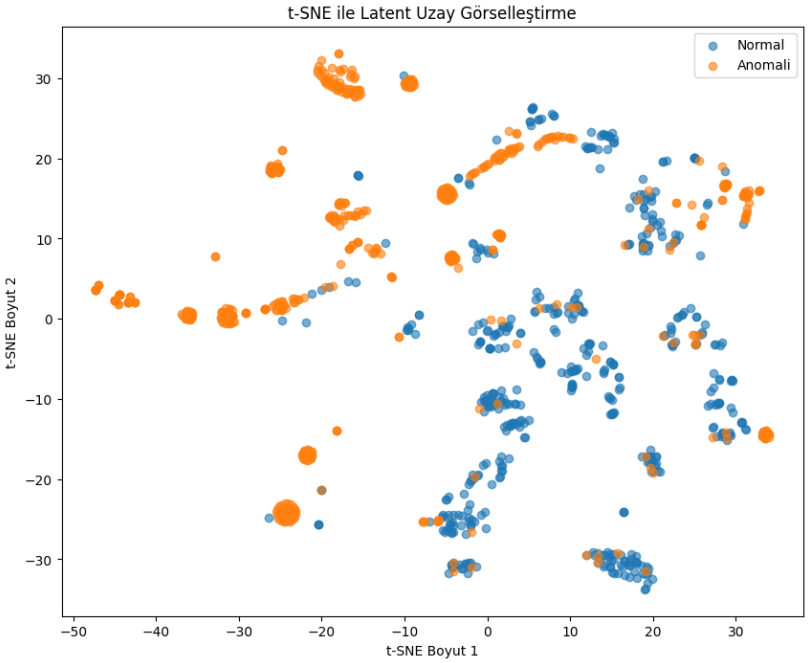
CSE-CIC-IDS2018 veri seti üzerinde ANFIS yönteminin çoklu etiket sınıflandırması için oluşturulan karmaşıklık matrisi Şekil 4.36'da detaylı bir şekilde incelenmiştir. Matriste, diyagonal elemanlar (örneğin, Normal: 1417, Bot: 1636, DDOS-HOIC: 1638) genellikle yüksek değerler göstererek doğru sınıflandırma oranlarının dominant olduğunu ortaya koymaktadır. Özellikle DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP, DoS-GoldenEye, DoS-Hulk) ve SSH-BruteForce gibi sınıflar neredeyse tamamen doğru tahmin edilmiştir (1636-1638 doğru tahmin). Ancak, Infilteration (589 doğru, 1042 yanlış) ve FTP-BruteForce (367 doğru, 1264 yanlış) gibi sınıflarda yanlış sınıflandırmalar dikkat çekmektedir. Bu durum, ANFIS yönteminin çoklu etiket sınıflandırmada çoğu anomali türünü başarılı bir şekilde tespit ettiğini, ancak Infilteration ve FTP-BruteForce gibi bazı sınıflarda ayrım zorluğu yaşadığını göstermektedir.

Çizelge 4.20. CSE-CIC-IDS2018 Veri Seti Üzerinde kullanılan Pekiştirmeli Öğrenme Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	Kesinlik	Duyarlılık	F-1 Skoru	Destek
İkili Etiket				
Normal	0.90	0.97	0.93	1638
Anomali	0.97	0.90	0.93	1638
Çoklu Etiket				
Normal	0.67	0.49	0.57	1637
Bot	0.96	0.97	0.97	1638
DDOS-HOIC	0.98	1.00	0.99	1638
DDoS-LOIC-HTTP	0.97	1.00	0.98	1638
DoS-GoldenEye	0.90	1.00	0.95	1638
DoS-Hulk	0.97	0.92	0.95	1637
DoS-SlowHTTPTest	0.75	0.80	0.78	1638
DoS-Slowloris	0.95	0.99	0.97	1638
FTP-BruteForce	0.78	0.76	0.77	1638
Infilteration	0.59	0.63	0.61	1637
SSH-Bruteforce	0.99	1.00	1.00	1637

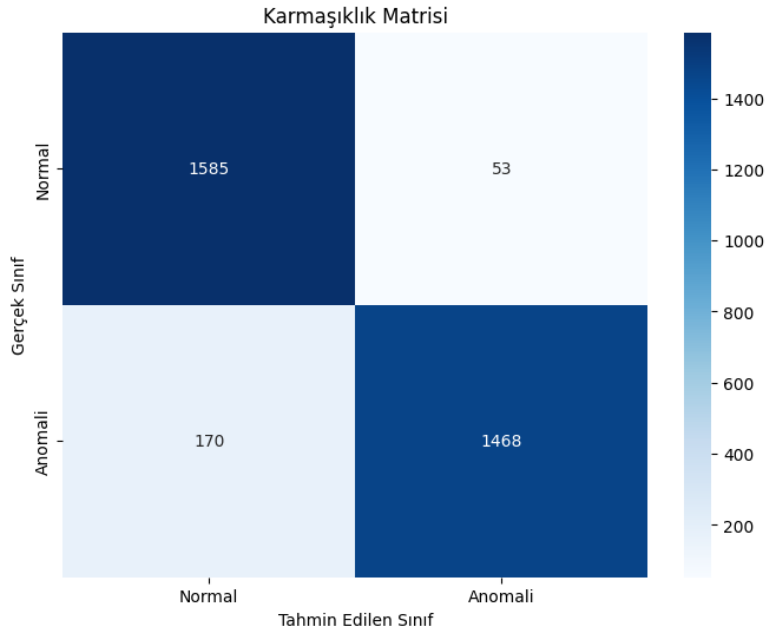
Çizelge 4.20, CSE-CIC-IDS2018 veri seti üzerinde Auto-Encoder + Pekiştirmeli Öğrenme DQN algoritması ile elde edilen sınıflandırma performans metriklerini sınıflar bazında incelemektedir. İkili etiket sınıflandırmada, normal sınıf için 0.90 kesinlik ve 0.97 duyarlılık, anomali sınıfında ise 0.97 kesinlik ve 0.90 duyarlılık ile her iki sınıf için F-1 skoru 0.93 olarak hesaplanmıştır. Çoklu etiket sınıflandırmada, SSH-Bruteforce sınıfı için 1.00 F-1 skoru ile mükemmel bir performans elde edilirken, DDOS-HOIC (0.99), DDoS-LOIC-HTTP (0.98), Bot (0.97) ve DoS-Slowloris (0.97) sınıfları da yüksek F-1 skorları sergilemiştir. Ancak, Normal sınıf için 0.67 kesinlik ve 0.49 duyarlılık ile 0.57 F-1 skoru, Infilteration sınıfı için ise 0.59 kesinlik ve 0.61 F-1 skoru gibi düşük değerler gözlemlenmiştir. Bu sonuçlar, pekiştirmeli öğrenme yönteminin ikili sınıflandırmada

daha dengeli bir performans sunduğunu, ancak çoklu etiket sınıflandırmada bazı sınıflarda, özellikle Normal ve Infilteration'da, performansın iyileştirilmesi gerektiğini göstermektedir.



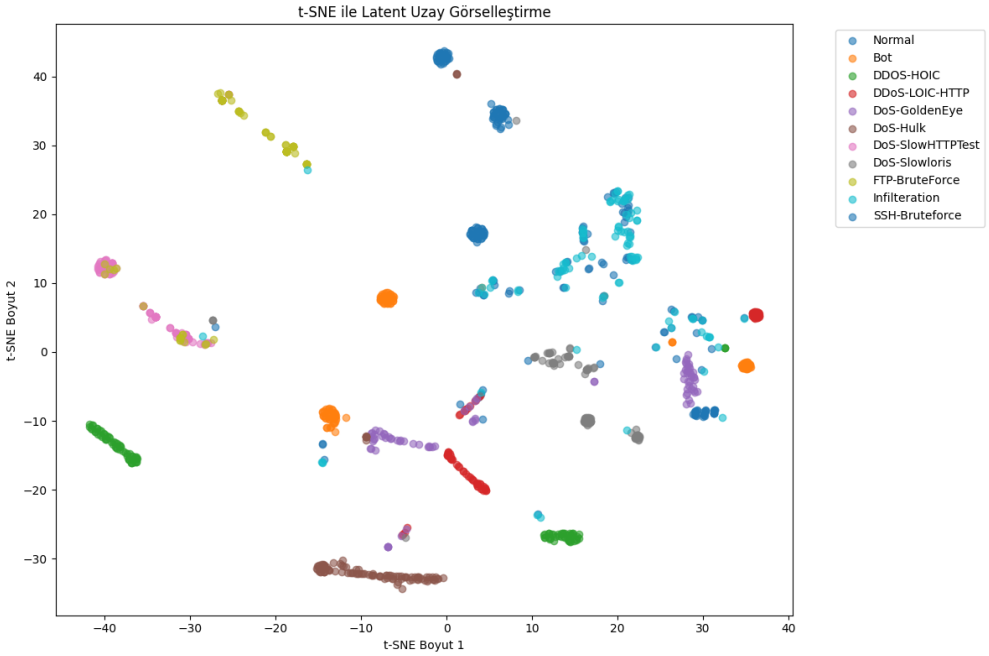
Şekil 4.37. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde pekiştirmeli öğrenme yönteminin ikili etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.37'de sunulmuştur. Grafikte, Normal sınıf mavi renkte yoğun bir şekilde merkezde kümelenmiş olarak yer alırken, Anomali sınıfı turuncu renkte daha dağınık bir şekilde dağılmıştır. Normal sınıfın kompakt bir yapı sergilemesi, pekiştirmeli öğrenme yönteminin bu sınıfı etkili bir şekilde ayırmada başarılı olduğunu göstermektedir. Anomali sınıfının ise farklı bölgelerde kümeler oluşturması, ikili etiket sınıflandırmasında anomalilerin ayrımında bazı zorluklar yaşandığını ve bu sınıfın heterojen bir yapıda olabileceğini düşündürmektedir. Bu görselleştirme, yöntemin ikili sınıflandırmada genel olarak iyi bir ayrım sağladığını, ancak Anomali sınıfındaki dağınıklığın performans üzerinde bir miktar etkisi olabileceğini ortaya koymaktadır.



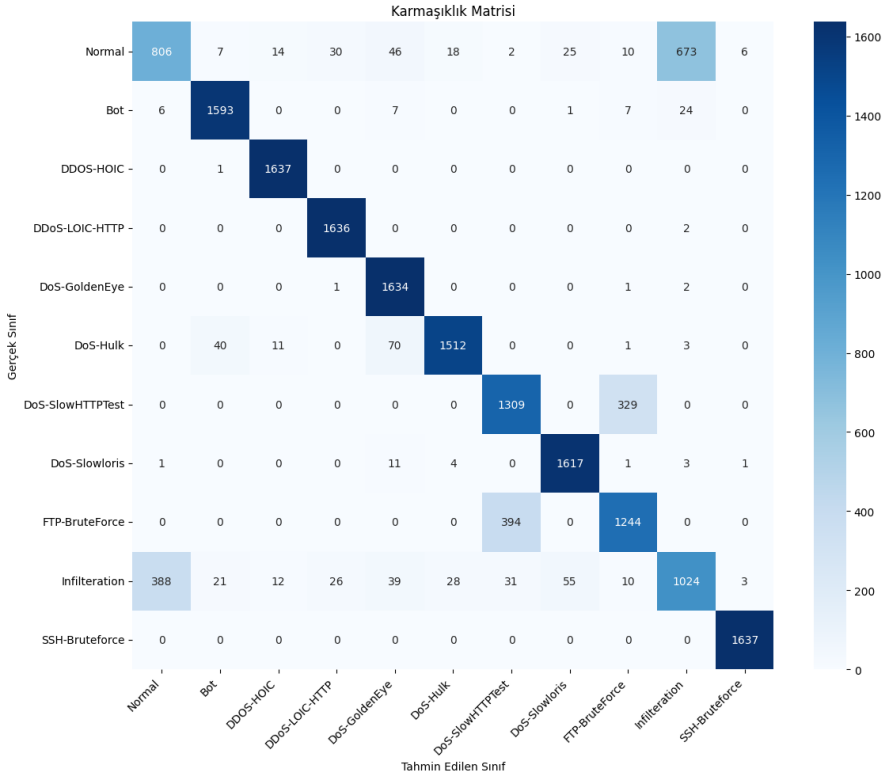
Şekil 4.38. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.38, CSE-CIC-IDS2018 veri seti üzerinde Pekiştirmeli Öğrenme yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasına ait karmaşıklık matrisini sunmaktadır. Matris, "Normal" ve "Anomali" olarak iki ana sınıfı içermektedir. "Normal" sınıfı için gerçeğe uygun (Gerçek Sınıf) ve tahmin edilen (Tahmin Edilen Sınıf) değerler arasında 1585 doğru tahmin bulunurken, 53 yanlış tahmin gözlemlenmiştir. "Anomali" sınıfında ise 170 örnek normal olarak yanlış tahmin edilmiş, 1468 örnek ise doğru şekilde anomali olarak sınıflandırılmıştır. Bu sonuçlar, modelin özellikle "Normal" sınıfını yüksek doğrulukla tanıdığını, ancak "Anomali" sınıfında bazı yanlış tahminlerle karşılaştığını göstermektedir.



Şekil 4.39. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket t-SNE grafiği

CSE-CIC-IDS2018 veri seti üzerinde pekiştirmeli öğrenme yönteminin çoklu etiket sınıflandırması için uygulanan t-SNE görselleştirme Şekil 4.39'da detaylı bir şekilde incelenmiştir. DDoS türleri (DDOS-HOIC, DDoS-LOIC-HTTP) ve DoS türleri (DoS-GoldenEye, DoS-Hulk) gibi bazı anomali sınıfları birbirine yakın kümeler halinde bulunurken, Bot ve Infilteration gibi sınıflar daha izole bölgelerde yer almıştır. Bu durum, pekiştirmeli öğrenme yönteminin çoklu etiket sınıflandırmada belirli anomali türlerini ayrıştırmada başarılı olduğunu, ancak bazı sınıflar arasında örtüşme veya ayrım zorluğu olabileceğini göstermektedir.



Şekil 4.40. CSE-CIC-IDS2018 veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.40, aynı veri seti üzerinde pekiştirmeli öğrenme yönteminin çoklu etiket sınıflandırmasına yönelik karmaşıklık matrisini içermektedir. "Normal" sınıfında 806 doğru tahmin öne çıkarken, "DDoS-HOIC" ve "DDoS-LOIC-HTTP" gibi saldırı türlerinde sırasıyla 1637 ve 1636 doğru tahmin elde edilmiştir. Bununla birlikte, "Infiltration" ve "SSH-BruteForce" gibi az örnek içeren sınıflarda yanlış tahmin oranları (örneğin, 1637 yanlış tahmin) dikkat çekmektedir. Bu durum, modelin yaygın saldırı türlerini daha iyi ayırt edebildiğini, ancak az temsil edilen sınıflarda performansının sınırlı olduğunu ortaya koymaktadır.

4.3. Edge-IIoTset Veri Seti ile Elde Edilen Bulgular

Edge-IIoTset veri seti, ağ tabanlı sistemlerdeki çeşitli saldırı türlerini kapsayan ve 13 sınıflı bir yapı sunan kapsamlı bir veri kümesi üzerinde gerçekleştirilen anomali tespiti çalışmalarını içermektedir. Bu alt bölümde, veri seti üzerinde uygulanan makine öğrenmesi modellerinin performansı, ikili ve çoklu sınıflandırma senaryolarında detaylı bir şekilde değerlendirilmiştir. Eğitim, doğrulama ve test kümelerindeki dengeli etiket

dağılımı, modellerin farklı saldırı türlerini sınıflandırma yeteneklerini test etmek için uygun bir zemin sağlamıştır. Bulgular, modellerin doğruluk ve maliyet metrikleri üzerinden karşılaştırılmasını sağlayarak, ağ tabanlı anomali tespiti için en uygun yaklaşımların belirlenmesine katkı sunmaktadır.

Çizelge 4.21. Edge-IIoTset Veri Setine Ait Öznitelik ve Sınıf Dağılımı

Kategori	**Bilgi / Açıklama**
Öznitelikler	http.request.version_0.0, http.request.method_0.0, http.request.version_0, http.request.method_0, http.request.version_HTTP/1.1, http.request.method_GET, tcp.flags.ack, http.referer_0.0, http.response, http.referer_0, icmp.checksum, icmp.seq_le, tcp.flags, tcp.ack_raw, tcp.checksum, http.content_length, tcp.connection.fin, udp.stream, tcp.connection.synack, tcp.len, http.request.method_TRACE, http.referer_127.0.0.1, tcp.ack, tcp.connection.syn, dns.qry.name, http.referer_() { ; } >[$($())] { echo 93e4r0-CVE-2014-6278: true; echo;echo; }, mqtt.conack.flags_1461589, http.request.version_Src=javascript:alert('Vulnerable')><Img Src=" HTTP/1.1, http.request.version_/etc/passwd|?data=Download HTTP/1.1, dns.qry.type
Öznitelik Sayısı	30 Öznitelik
Saldırı Haritası	{'Normal': 0, 'DDoS_UDP': 1, 'SQL_injection': 2, 'Backdoor': 3, 'Ransomware': 4, 'Uploading': 5, 'DDoS_HTTP': 6, 'DDoS_TCP': 7, 'Password': 8, 'Port_Scanning': 9, 'XSS': 10, 'Vulnerability_scanner': 11, 'DDoS_ICMP': 12} – Saldırılar 13 sınıfa ayrılmıştır.
Sınıf Sayısı	13 Etiket
Eğitim Etiket Dağılımı	[7751 7751 7751 7751 7751 7751 7751 7751 7751 7752 7752 7752 7751]– Her sınıf için dengeli örnekleme yapılmıştır.

Doğrulama Etiket Dağılımı	[969 969 969 969 969 969 969 969 969 969 968 968 969 969] – Doğrulama kümesindeki her sınıfın örnek sayısı.
Test Etiket Dağılımı	[969 969 969 969 969 969 969 969 969 969 969 969 968 969]– Test kümesindeki her sınıfın örnek sayısı.
Veri Boyutları	Eğitim: (100,766x 30), Doğrulama: (12,595 x 30), Test: (12,596 x 30) – Toplamda 125,957 örnek kullanılmıştır.

Edge-IIoTset veri seti, 30 öznitelik içeren ve ağ trafiği ile ilgili spesifik ölçümleri temsil eden sadeleştirilmiş bir veri kümesidir. Öznitelikler arasında "http.request.method_GET", "tcp.flags.ack", "icmp.checksum", "dns.qry.name" gibi HTTP, TCP, ICMP ve DNS protokolleriyle ilişkili özellikler yer almaktadır. Saldırı haritası, "Normal" ve 12 farklı saldırı türü ("DDoS_UDP", "SQL_injection", "Backdoor", "Ransomware", "Uploading", "DDoS_HTTP", "DDoS_TCP", "Password", "Port_Scanning", "XSS", "Vulnerability_scanner", "DDoS_ICMP") olmak üzere 13 sınıfa ayrılmıştır. Bu, veri setinin çoklu sınıflandırma problemleri için oldukça karmaşık ve zorlayıcı bir yapı sunduğunu göstermektedir. Eğitim kümesi 100,766 örnek, doğrulama kümesi 12,595 örnek ve test kümesi 12,596 örnek içermektedir. Etiket dağılımı, her sınıf için dengeli bir şekilde düzenlenmiş olup, eğitim kümesinde her sınıf yaklaşık 7,751-7,752 örnek, doğrulama ve test kümelerinde ise yaklaşık 968-969 örnek içermektedir. Bu dengeli yapı, modellerin her sınıf için adil bir şekilde eğitilmesini ve değerlendirilmesini sağlamıştır. Öznitelik sayısının 30 olması, veri setinin işleme yükünü bir miktar azaltırken, 13 sınıflı yapısı modellerin genelleştirme kapasitesini sınayan karmaşık bir senaryo sunmaktadır.

Çizelge 4.22. Edge-IIoTset Veri Seti Üzerinde Makine Öğrenmesi Modellerinin Performans Karşılaştırması

Model Tipi	**Model ismi**	**İsabetlilik % (Doğrulama) : İkili Etiket**	**İsabetlilik % (Test) : İkili Etiket**	**Toplam Maliyet (Doğrulama) : İkili**	**Toplam Maliyet (Test) : İkili**

		/ Çoklu Etiket	**/ Çoklu Etiket**	**Etiket / Çoklu Etiket**	**Etiket / Çoklu Etiket**
Tree	Fine Tree	100 / 91.24	100 / 90.77	0 / 9929	0 / 1163
Tree	Medium Tree	100 / 64.38	100 / 63.23	0 / 40374	0 / 4631
Tree	Coarse Tree	100 / 37.38	100/37.29	0/70988	0/7898
Discriminant	Linear Discriminant	99.91 / 51.31	99.95/50.89	77/55192	5/6185
Logistic Regression	Logistic Regression	100 / -	100 / -	/ -	/ -
Naive Bayes	Gaussian Naive Bayes	98.26/29.08	98.31/29.44	1568/80399	169/8887
SVM	Medium Gaussian SVM	100/78.86	100/78.72	0/23965	0/2680
KNN	Fine KNN	100/78.11	100/77.86	0/24818	0/2789
KNN	Medium KNN	100/78.06	100/78.09	0/24876	0/2759
KNN	Coarse KNN	100/76.62	100/76.79	0/26503	0/2923
KNN	Cosine KNN	100/78.09	100/78.09	0/24837	0/2759
KNN	Weighted KNN	100/78.35	100/78.24	0/24547	0/2741
Ensemble	Boosted Trees	71.17/82.88	70.88/82.55	25949/19413	2912/2198
Ensemble	Bagged Trees	100/92.31	100/92.12	0/8718	0/993

Ensemble	Subspace Discriminant	99.99/55.45	100/54.83	2/50502	0/5689
Ensemble	RUSBoosted Trees	69.49/63.62	69.6/62.95	27455/41240	3040/4666

Edge-IIoTset veri seti üzerinde test edilen makine öğrenmesi modelleri, ikili ve çoklu sınıflandırma senaryolarında dikkat çekici performans farklılıkları sergilemiştir. Ensemble yöntemlerden "Bagged Trees", doğrulama kümesinde %100 (ikili) ve %92.31 (çoklu), test kümesinde ise %100 (ikili) ve %92.12 (çoklu) doğruluk oranlarıyla en yüksek performansı göstermiştir. Bu modelin düşük toplam maliyeti (doğrulama: 0/8718, test: 0/993), ağ tabanlı karmaşık saldırı türlerini etkili bir şekilde sınıflandırabildiğini ve genelleştirme yeteneğinin üstün olduğunu ortaya koymaktadır. "Fine Tree" modeli de %100 (ikili, test) ve %90.77 (çoklu, test) doğruluk oranlarıyla güçlü bir performans sergilemiş, özellikle ikili sınıflandırmada mükemmel sonuçlar üretmiştir.

Bununla birlikte, "Naive Bayes" modeli, %98.31 (ikili, test) ve %29.44 (çoklu, test) doğruluk oranlarıyla çoklu sınıflandırmada oldukça düşük bir performans sergilemiş ve yüksek maliyet değerleri (doğrulama: 1568/80399, test: 169/8887) ile hesaplama verimliliğinin sınırlı olduğunu göstermiştir. Bu durum, Naive Bayes'in öznitelikler arasındaki bağımlılıkları modellemede ve çok sınıflı problemlerde yetersiz kaldığını düşündürmektedir. KNN tabanlı modeller arasında "Weighted KNN" ve "Cosine KNN", %100 (ikili, test) ve sırasıyla %78.24 ve %78.09 (çoklu, test) doğruluk oranlarıyla iyi sonuçlar üretmiş, ancak çoklu sınıflandırmada "Bagged Trees" gibi ensemble modellere kıyasla daha düşük performans göstermiştir. "Boosted Trees" ve "RUSBoosted Trees" modelleri, ikili sınıflandırmada sırasıyla %70.88 ve %69.6 (test) doğruluk oranlarıyla beklenenden düşük performans sergilemiş, bu da bu modellerin veri setindeki bazı sınıfları ayırt etmede zorlandığını göstermektedir.

Genel olarak, ensemble ve ağaç tabanlı modeller, Edge-IIoTset veri setinde ikili sınıflandırmada mükemmel sonuçlar üretirken, çoklu sınıflandırma senaryosunda da yüksek doğruluk oranlarıyla öne çıkmıştır. Çoklu sınıflandırmada doğruluk oranlarının ikili sınıflandırmaya kıyasla daha düşük olması, 13 sınıflı yapının modeller için zorlayıcı

olduğunu ve sınıflar arasında örtüşmelerin mevcut olabileceğini göstermektedir. Naive Bayes ve bazı ensemble modellerin düşük performansları, bu modellerin karmaşık ağ veri setlerinde sınırlı kaldığını ortaya koymaktadır.

Çizelge 4.23. Edge-IIoTset Veri Seti Üzerinde Kullanılan Derin Öğrenme Tabanlı Yöntemler

Yöntem	**İsabetlilik (İkili/Çoklu etiket)**	**Kesinlik (İkili/Çoklu etiket)**	**Duyarlılık (İkili/Çoklu etiket)**	**F-1 Skoru (İkili/Çoklu etiket)**	**MCC (İkili/Çoklu etiket)**
CNN	1.00 / 0.7928	1.00 / 0.8232	1.00 / 0.7928	1.00 / 0.7902	1.00 / 0.7792
LSTM	1.00 /0.7973	1.00 /0.8607	1.00 /0.7973	1.00 /0.7877	1.00 /0.7873

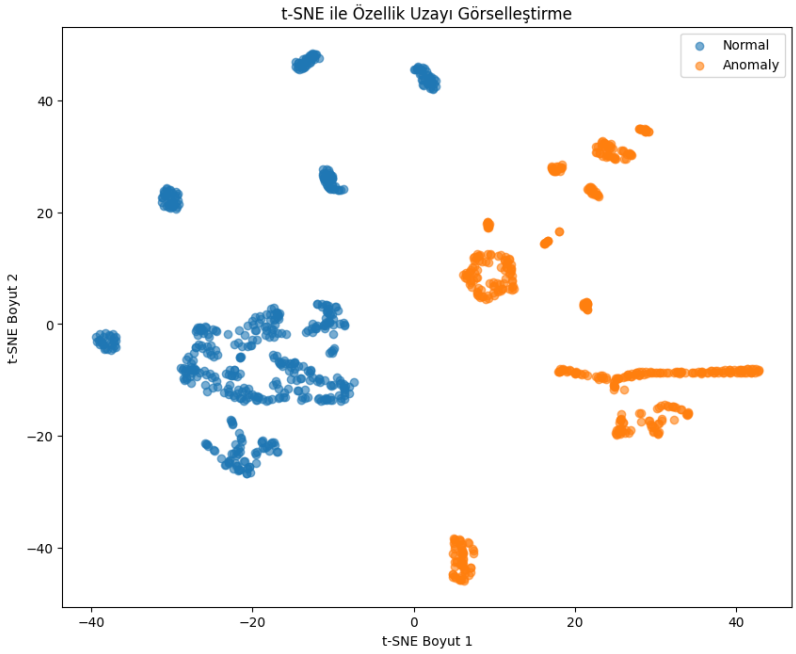
Edge-IIoTset veri seti üzerinde derin öğrenme tabanlı yöntemlerin performansını değerlendirmek amacıyla Çizelge 4.23'te sunulan metrikler incelenmiştir. Bu çizelgede, CNN ve LSTM algoritmalarının ikili ve çoklu etiket sınıflandırmalarındaki performansları karşılaştırılmıştır. CNN yöntemi, ikili etiket sınıflandırmada 1.00 isabetlilik, kesinlik, duyarlılık, F-1 skoru ve MCC ile kusursuz bir performans sergilerken, çoklu etiket sınıflandırmada 0.7928 isabetlilik, 0.8232 kesinlik ve 0.7792 MCC değerleriyle daha düşük ancak yine de dikkate değer bir başarı göstermiştir. LSTM yöntemi ise ikili etiket sınıflandırmada aynı şekilde 1.00 değerlerine ulaşmış, çoklu etiket sınıflandırmada ise 0.7973 isabetlilik, 0.8607 kesinlik ve 0.7873 MCC ile CNN'ye kıyasla biraz daha iyi bir performans sunmuştur. Bu sonuçlar, her iki yöntemin ikili sınıflandırmada mükemmel sonuçlar verdiğini, ancak çoklu etiket sınıflandırmada LSTM'nin biraz daha yüksek kesinlik sağladığını göstermektedir.

Çizelge 4.24. Edge-IIoTset Veri Seti Üzerinde Kullanılan CNN Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				

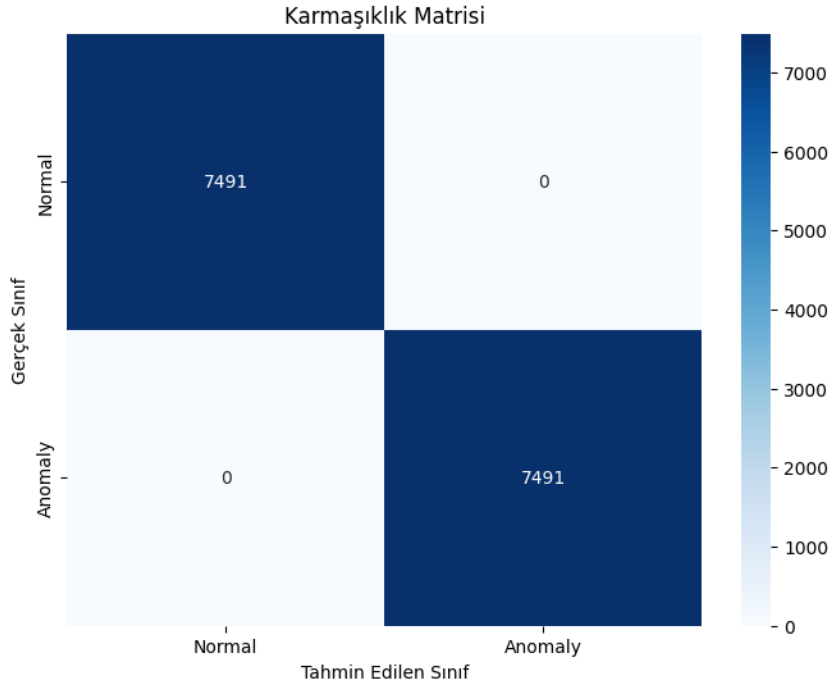
Normal	1.00	1.00	1.00	1638
Anomali	0.99	0.91	0.95	1638
Çoklu Etiket				
Backdoor	0.96	0.93	0.95	969
DDoS_HTTP	0.86	0.62	0.72	969
DDoS_ICMP	1.00	1.00	1.00	969
DDoS_TCP	1.00	0.57	0.73	969
DDoS_UDP	1.00	1.00	1.00	969
Normal	1.00	0.90	0.94	969
Password	0.54	0.30	0.39	969
Port_Scanning	0.68	1.00	0.81	969
Ransomware	0.89	0.97	0.93	969
SQL_injection	0.43	0.75	0.55	969
Uploading	0.71	0.51	0.59	969
Vulnerability_scanner	1.00	0.86	0.92	968
XSS	0.64	0.90	0.75	969

Çizelge 4.24, Edge-IIoTset veri seti üzerinde CNN algoritması ile elde edilen sınıflandırma performans metriklerini sınıflar bazında detaylandırmaktadır. İkili etiket sınıflandırmada, Normal sınıf için 1.00 kesinlik, duyarlılık ve F-1 skoru ile mükemmel bir performans elde edilmiş, Anomali sınıfında ise 0.99 kesinlik, 0.91 duyarlılık ve 0.95 F-1 skoru raporlanmıştır. Çoklu etiket sınıflandırmada, DDoS_ICMP, DDoS_UDP ve Normal sınıfları için 1.00 kesinlik ve yüksek F-1 skorları (0.94-1.00) dikkat çekerken, Backdoor (0.95 F-1) ve Ransomware (0.93 F-1) sınıfları da yüksek performans göstermiştir. Ancak, Password (0.39 F-1), SQL_injection (0.55 F-1) ve Uploading (0.59 F-1) sınıflarında düşük F-1 skorları elde edilmiştir. Bu sonuçlar, CNN algoritmasının belirli anomali türlerinde (örneğin, DDoS_ICMP ve DDoS_UDP) oldukça başarılı olduğunu, ancak Password ve SQL_injection gibi sınıflarda performansın iyileştirilmesi gerektiğini ortaya koymaktadır.



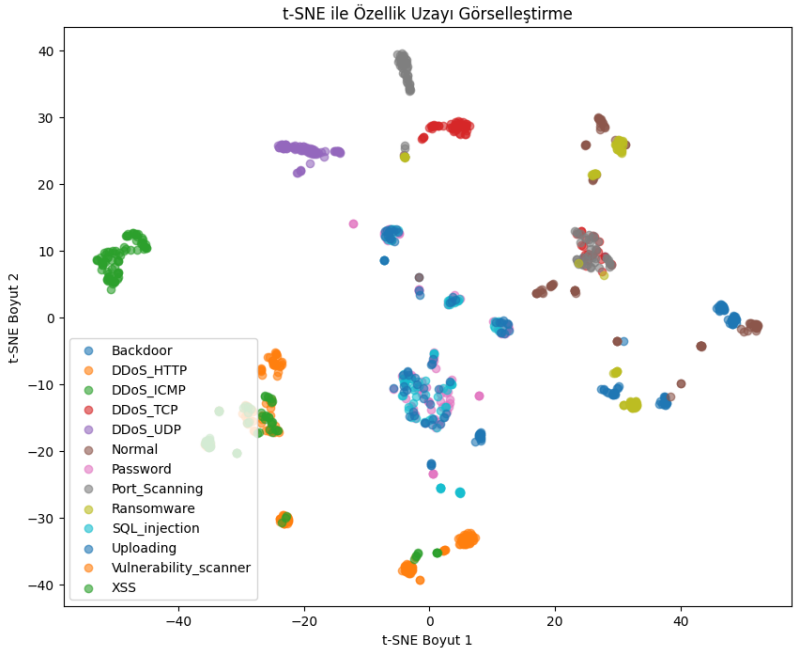
Şekil 4.41. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin ikili etiket t-SNE grafiği

Şekil 4.41, Edge-IIoTset veri seti üzerinde CNN yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasına ait t-SNE Özellik Uzayı Görselleştirme grafiğini sunmaktadır. Grafikte, "Normal" sınıfı mavi renkli noktalarla yoğun bir şekilde kümelenirken, "Anomali" sınıfı turuncu renkli noktalarla ayrık gruplar halinde dağılmıştır. Bu durum, modelin "Normal" ve "Anomali" sınıflarını belirli bir ölçüde ayırabildiğini, ancak bazı kesişim alanlarında sınıflar arası karışım olduğunu göstermektedir.



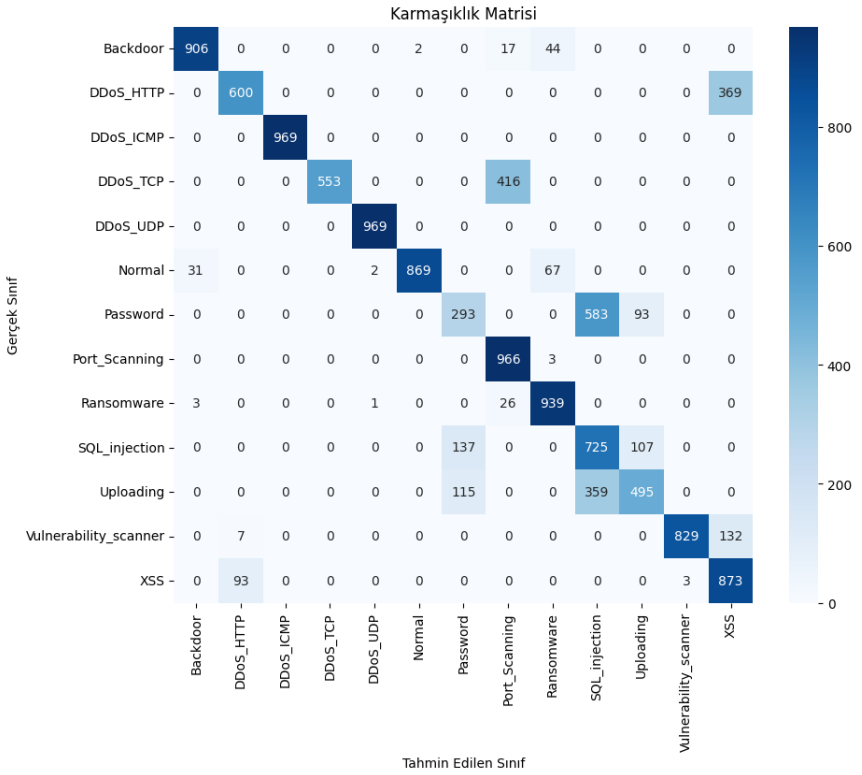
Şekil 4.42. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.42, Edge-IIoTset veri seti üzerinde CNN yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasına ait karmaşıklık matrisini sunmaktadır. "Normal" sınıfında 7491 doğru tahmin elde edilirken, "Anomali" sınıfında da 7491 doğru tahmin yapılmıştır. Her iki sınıf için sıfır yanlış tahmin bulunması, modelin ikili sınıflandırmada mükemmele yakın bir performans sergilediğini göstermektedir.



Şekil 4.43. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin çoklu etiket t-SNE grafiği

Şekil 4.43, aynı veri seti üzerinde CNN yönteminin çoklu etiket sınıflandırmasına yönelik t-SNE grafiğini içermektedir. Her bir sınıf, belirli kümeler halinde görselleştirilmiş olup, özellikle "Normal" ve "DDoS" türleri arasında belirgin ayrışmalar gözlemlenmektedir. Bununla birlikte, "Password" ve "Port_Scanning" gibi bazı sınıflar daha dağınık bir yapı sergileyerek, modelin bu az temsil edilen sınıfları ayırt etme performansının sınırlı olabileceğini işaret etmektedir.



Şekil 4.44. Edge-IIoTset veri seti üzerinde uygulanan CNN yönteminin çoklu etiket karmaşıklık matrisi

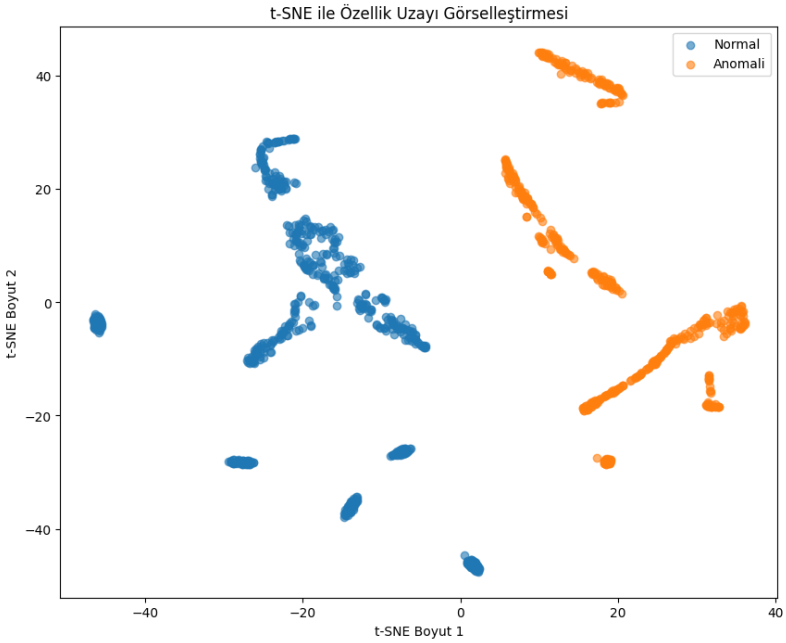
Şekil 4.44, aynı veri seti üzerinde CNN yönteminin çoklu etiket sınıflandırmasına yönelik karmaşıklık matrisini içermektedir. "Normal" sınıfında 869 doğru tahmin öne çıkarken, "DDoS" türleri (örneğin, DDoS_HTTP için 600, DDoS_TCP için 553) ve "XSS" için 873 doğru tahmin dikkat çekmektedir. Bununla birlikte, bazı sınıflar arasında karışıklıklar (örneğin, "Backdoor" ile "XSS" arasında 93 yanlış tahmin) gözlemlenmiş, bu da modelin az temsil edilen sınıflarda ayrım performansının sınırlı olabileceğini işaret etmektedir.

Çizelge 4.25. Edge-IIoTset Veri Seti Üzerinde Kullanılan LSTM Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	**Kesinlik**	**Duyarlılık**	**F-1 Skoru**	**Destek**
İkili Etiket				
Normal	1.00	1.00	1.00	1638
Anomali	1.00	1.00	1.00	1638

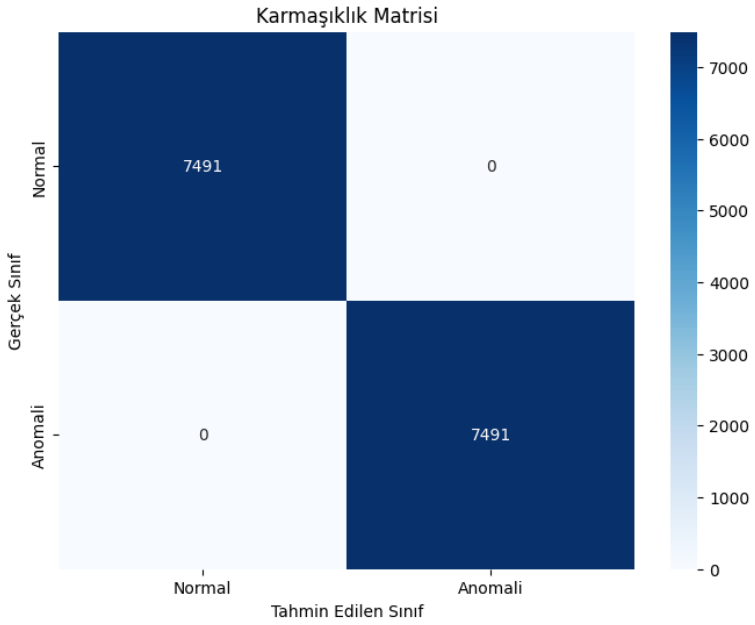
Çoklu Etiket				
Backdoor	0.97	0.93	0.95	969
DDoS_HTTP	0.86	0.62	0.72	969
DDoS_ICMP	1.00	1.00	1.00	969
DDoS_TCP	1.00	0.57	0.73	969
DDoS_UDP	1.00	1.00	1.00	969
Normal	1.00	0.91	0.95	969
Password	0.43	0.91	0.58	969
Port_Scanning	0.68	1.00	0.81	969
Ransomware	0.90	0.97	0.93	969
SQL_injection	1.00	0.17	0.29	969
Uploading	0.72	0.51	0.60	969
Vulnerability_scanner	1.00	0.86	0.92	968
XSS	0.64	0.91	0.75	969

Çizelge 4.25, Edge-IIoTset veri seti üzerinde LSTM algoritması ile elde edilen sınıflandırma performans metriklerini sunmaktadır. İkili etiket sınıflandırmada, hem Normal hem de Anomali sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.00 olarak hesaplanarak kusursuz bir performans sergilenmiştir. Çoklu etiket sınıflandırmada, DDoS_ICMP, DDoS_UDP ve SSH-Bruteforce sınıfları için 1.00 kesinlik ve duyarlılık ile 1.00 F-1 skoru elde edilirken, Backdoor (0.95 F-1), Ransomware (0.93 F-1) ve Vulnerability_scanner (0.92 F-1) sınıfları da yüksek performans göstermiştir. Bununla birlikte, SQL_injection sınıfı için 0.17 duyarlılık ve 0.29 F-1 skoru, Password sınıfı için 0.43 kesinlik ve 0.58 F-1 skoru gibi düşük değerler dikkat çekmektedir. Bu sonuçlar, LSTM algoritmasının ikili sınıflandırmada mükemmel bir başarı sağladığını, ancak çoklu etiket sınıflandırmada özellikle SQL_injection ve Password sınıflarında performansın geliştirilmesi gerektiğini göstermektedir.



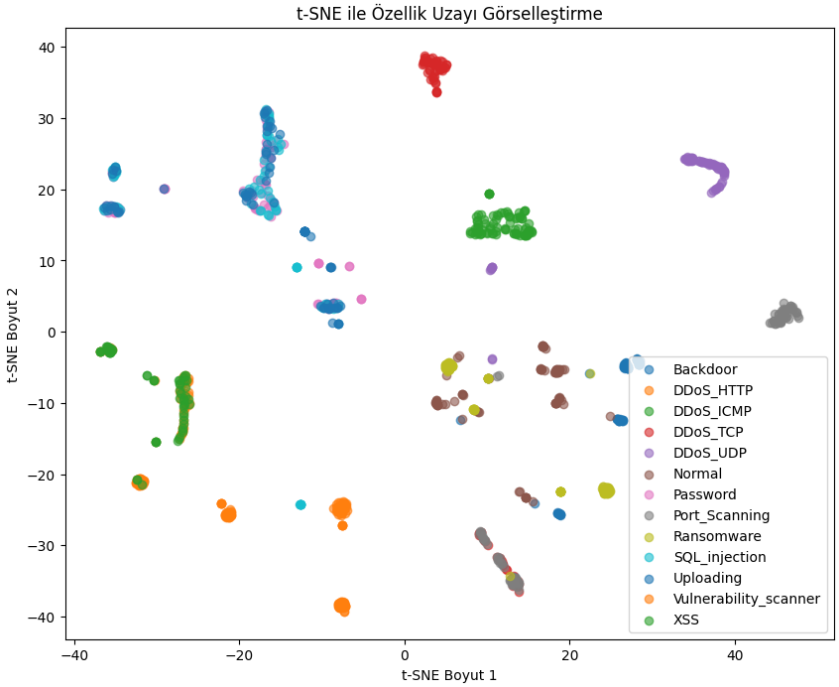
Şekil 4.45. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin ikili etiket t-SNE grafiği

Şekil 4.45, Edge-IIoTset veri seti üzerinde LSTM yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasının t-SNE görselleştirmesini sunmaktadır. "Normal" sınıfı, kompakt bir küme şeklinde kümelenirken, "Anomali" sınıfı daha dağınık bir dağılım sergilemektedir. Bu ayrım, LSTM modelinin ikili sınıflandırma görevinde "Normal" ve "Anomali" durumlarını etkili bir şekilde ayırt edebildiğini ve modelin veri setindeki temel yapısal farklılıkları yakalayabildiğini göstermektedir.



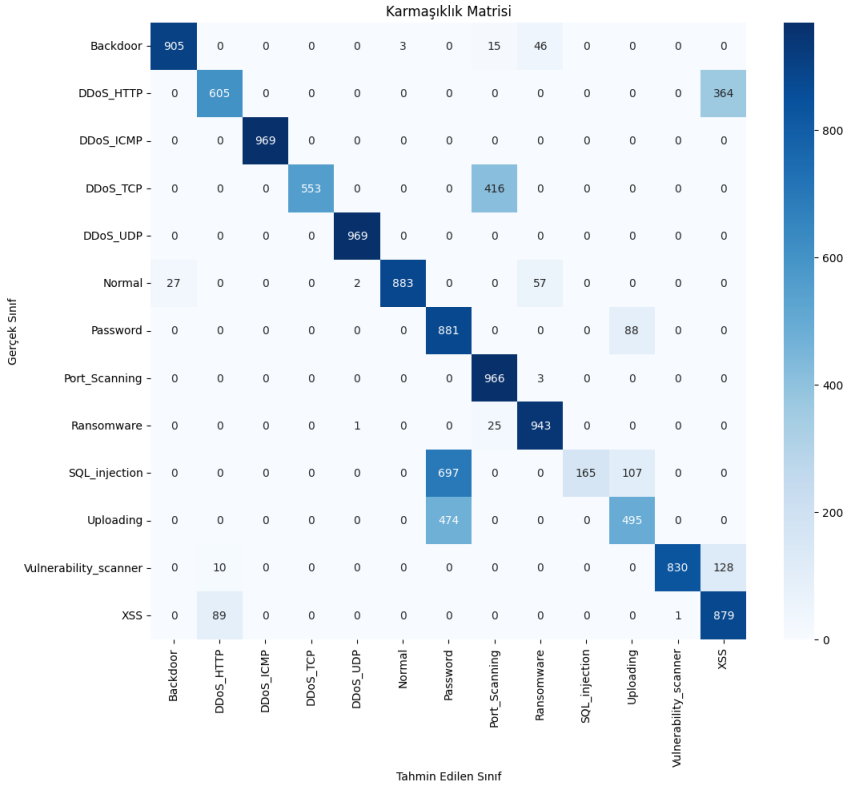
Şekil 4.46. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.46'a göre; "Normal" sınıfı için 7491 örnek doğru tahmin edilmiş, "Anomali" sınıfı için de 7491 örnek doğru sınıflandırılmıştır. Yanlış sınıflandırma oranları sıfır olarak raporlanmıştır, bu da modelin her iki sınıfı da mükemmel bir doğrulukla ayırt edebildiğini ve ikili sınıflandırma görevinde olağanüstü bir performans sergilediğini göstermektedir. Bu sonuç, LSTM modelinin veri setindeki ikili ayrımı etkin bir şekilde gerçekleştirdiğini kanıtlamaktadır.



Şekil 4.47. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket t-SNE grafiği

Şekil 4.47, her bir sınıfın veri noktalarının farklı bölgelerde kümelendiğini ve bazı sınıflar arasında örtüşme olduğunu ortaya koymaktadır. Örneğin, Backdoor ve DDoS_TCP gibi sınıflar daha belirgin kümeler oluştururken, SQL_Injection ve Uploading gibi sınıflar daha dağınık bir dağılım sergilemektedir. Bu durum, LSTM modelinin çoklu etiket sınıflandırmasında sınıf ayrımında genel olarak başarılı olduğunu, ancak az temsil edilen veya benzer özelliklere sahip sınıflarda ayrım zorluğu yaşadığını göstermektedir.



Şekil 4.48. Edge-IIoTset veri seti üzerinde uygulanan LSTM yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.48'e göre, XSS sınıfı için 879, Backdoor için 905 doğru tahmin elde edilmiştir. Yanlış sınıflandırmalar arasında, XSS sınıfının 89 örneği Vulnerability_Scanner olarak yanlış tahmin edilmesi dikkat çekmektedir. Bunun yanı sıra, SQL_Injection sınıfında 697 doğru tahmine karşılık 165 örnek Uploading olarak yanlış sınıflandırılmıştır. Bu sonuçlar, modelin genel olarak çoklu etiket sınıflandırmasında başarılı olduğunu, ancak bazı benzer özelliklere sahip sınıflar arasında ayrım zorluğu yaşadığını ortaya koymaktadır.

Çizelge 4.26. Edge-IIoTset Veri Seti Üzerinde Kullanılan Yumuşak Hesaplama Tabanlı Yöntemler

Yöntem	**İsabetlilik (İkili/Çoklu etiket)**	**Kesinlik (İkili/Çoklu etiket)**	**Duyarlılık (İkili/Çoklu etiket)**	**F-1 Skoru (İkili/Çoklu etiket)**	**MCC (İkili/Çoklu etiket)**

GA	1.0000 / 0.8992	1.0000 / 0.9086	1.0000 / 0.8992	1.0000 / 0.8990	1.0000 / 0.8908

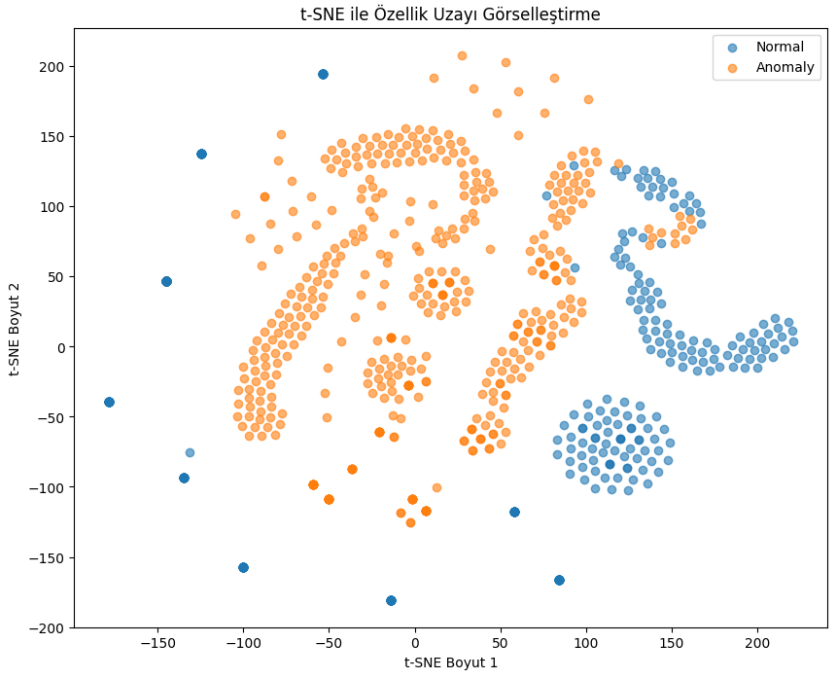
Edge-IIoTset veri seti üzerinde yumuşak hesaplama tabanlı yöntemlerin performansını değerlendirmek amacıyla Çizelge 4.26'da sunulan metrikler incelenmiştir. Bu çizelgede, GA yönteminin ikili ve çoklu etiket sınıflandırmalarındaki performansı detaylı bir şekilde ele alınmıştır. GA yöntemi, ikili etiket sınıflandırmada 1.0000 isabetlilik, kesinlik, duyarlılık, F-1 skoru ve MCC ile kusursuz bir performans sergilemiştir. Çoklu etiket sınıflandırmada ise 0.8992 isabetlilik, 0.9086 kesinlik, 0.8992 duyarlılık, 0.8990 F-1 skoru ve 0.8908 MCC değerleri elde edilmiştir. Bu sonuçlar, GA yönteminin ikili sınıflandırmada mükemmel bir başarı sağladığını ve çoklu etiket sınıflandırmada da yüksek ve dengeli bir performans sunduğunu göstermektedir.

Çizelge 4.27. Edge-IIoTset Veri Seti Üzerinde Kullanılan GA Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	Kesinlik	Duyarlılık	F-1 Skoru	Destek
İkili Etiket				
Normal	1.00	1.00	1.00	7491
Anomali	1.00	1.00	1.00	7491
Çoklu Etiket				
Backdoor	0.90	0.66	0.76	969
DDoS_HTTP	0.87	0.88	0.87	969
DDoS_ICMP	1.00	1.00	1.00	969
DDoS_TCP	1.00	1.00	1.00	969
DDoS_UDP	1.00	1.00	1.00	969
Normal	1.00	0.94	0.97	969
Password	0.75	0.91	0.82	969
Port_Scanning	0.91	1.00	0.96	969
Ransomware	0.71	0.87	0.78	969
SQL_injection	1.00	0.72	0.84	969
Uploading	0.82	0.87	0.84	969

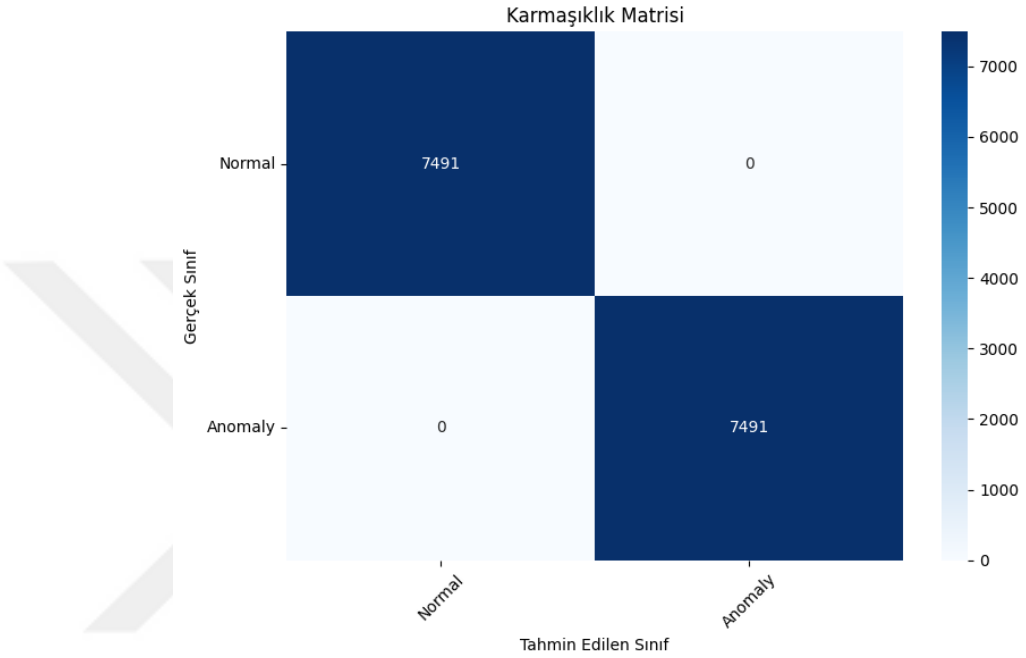
Vulnerability_scanner	0.99	0.90	0.94	968
XSS	0.87	0.94	0.90	969

Çizelge 4.27, Edge-IIoTset veri seti üzerinde GA algoritması ile elde edilen sınıflandırma performans metriklerini sınıflar bazında sunmaktadır. İkili etiket sınıflandırmada, hem Normal hem de Anomali sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.00 olarak hesaplanarak olağanüstü bir performans elde edilmiştir. Çoklu etiket sınıflandırmada, DDoS_ICMP, DDoS_TCP ve DDoS_UDP sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.00 gibi mükemmel değerlere ulaşırken, Normal (0.97 F-1), Port_Scanning (0.96 F-1) ve Vulnerability_scanner (0.94 F-1) sınıfları da yüksek performans göstermiştir. Ancak, Backdoor (0.66 duyarlılık, 0.76 F-1), Ransomware (0.71 kesinlik, 0.78 F-1) ve SQL_injection (0.72 duyarlılık, 0.84 F-1) sınıflarında nispeten daha düşük değerler gözlemlenmiştir. Bu sonuçlar, GA algoritmasının özellikle belirli anomali türlerinde (DDoS türleri) oldukça başarılı olduğunu, ancak Backdoor ve Ransomware gibi sınıflarda performansın geliştirilmeye açık olduğunu ortaya koymaktadır.



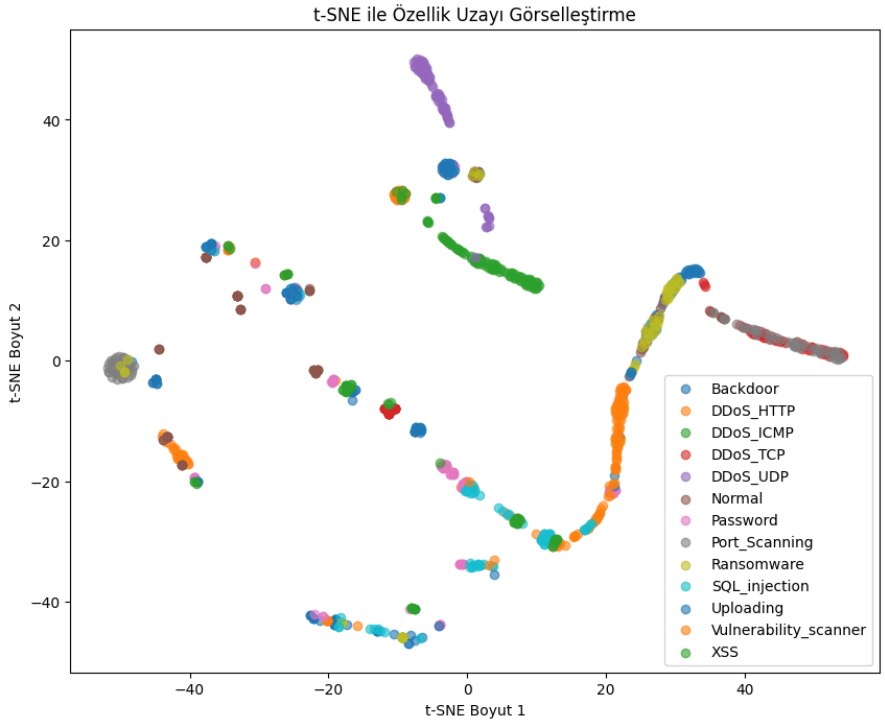
Şekil 4.49. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin ikili etiket t-SNE grafiği

Şekil 4.49'ye göre, "Normal" sınıfı yoğun bir küme oluştururken, "Anomali" sınıfı daha dağınık bir dağılım sergilemektedir. Bu ayrım, GA yönteminin ikili sınıflandırma görevinde "Normal" ve "Anomali" durumlarını etkili bir şekilde ayırt edebildiğini ve veri setindeki temel yapısal farklılıkları yakalayabildiğini ortaya koymaktadır.



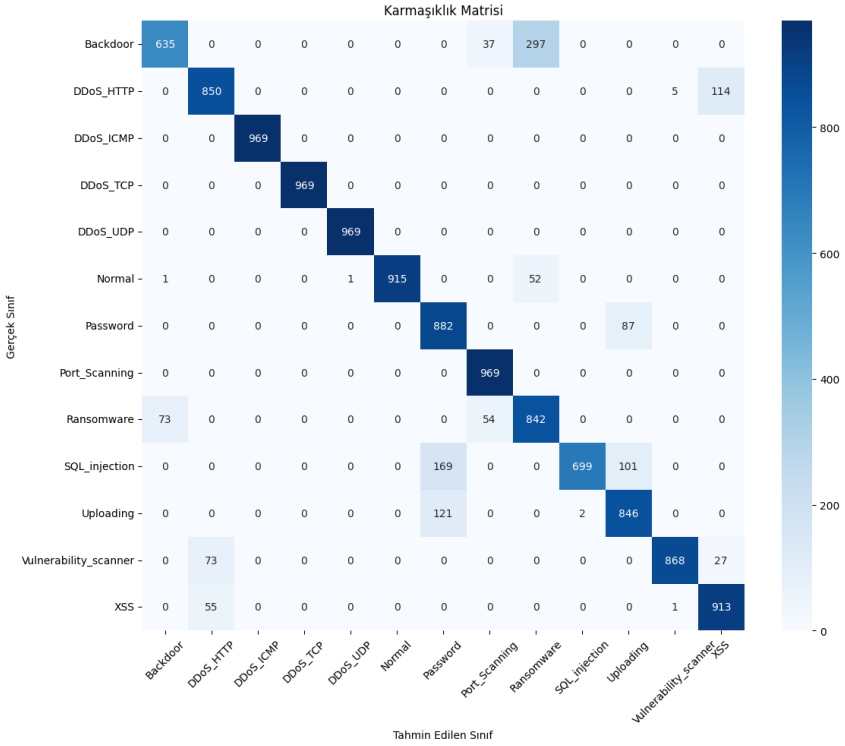
Şekil 4.50. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.50, Edge-IIoTset veri seti üzerinde GA yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasının karmaşıklık matrisini göstermektedir. "Normal" sınıfı için 7491 örnek doğru tahmin edilmiş, "Anomali" sınıfı için de 7491 örnek doğru sınıflandırılmıştır. Yanlış sınıflandırma oranlarının sıfır olması, GA yönteminin her iki sınıfı mükemmel bir doğrulukla ayırt edebildiğini ve ikili sınıflandırma görevinde üstün bir performans sergilediğini kanıtlamaktadır.



Şekil 4.51. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin çoklu etiket t-SNE grafiği

Şekil 4.51, her bir sınıfın veri noktalarının farklı bölgelerde kümelendiğini, ancak bazı sınıflar arasında örtüşme olduğunu göstermektedir. Backdoor ve DDoS_TCP gibi sınıflar belirgin kümeler oluştururken, SQL_Injection ve Uploading gibi sınıflar daha dağınık bir dağılım sergilemektedir. Bu durum, GA yönteminin çoklu etiket sınıflandırmasında genel olarak başarılı olduğunu, ancak benzer özelliklere sahip sınıflarda ayrım zorluğu yaşadığını ifade etmektedir.



Şekil 4.52. Edge-IIoTset veri seti üzerinde uygulanan GA yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.52 üzerinden incelendiğinde, GA yöntemiyle gerçekleştirilen çoklu etiket sınıflandırmasının karmaşıklık matrisi, Backdoor için 635, XSS için 913 doğru tahmini ortaya koymaktadır. Yanlış sınıflandırmalar arasında, XSS'nin 55 örneği Vulnerability_Scanner olarak yanlış tahmin edilmesi dikkat çekerken, SQL_Injection'da 699 doğru tahmine karşılık 101 örnek Uploading olarak yanlış sınıflandırılmıştır. Bu sonuçlar, GA yönteminin çoklu etiket sınıflandırmasında genel olarak başarılı olduğunu, ancak bazı sınıflar arasında ayrım zorluğu yaşadığını göstermektedir.

Çizelge 4.28. Edge-IIoTset Veri Seti Üzerinde Kullanılan Hibrit Tabanlı Yöntemler

Yöntem	**İsabetlilik (İkili/Çoklu etiket)**	**Kesinlik (İkili/Çoklu etiket)**	**Duyarlılık (İkili/Çoklu etiket)**	**F-1 Skoru (İkili/Çoklu etiket)**	**MCC (İkili/Çoklu etiket)**
ANFIS + GA	0.8191/ 0.7923	0.7343/ 0.8165	1.0000/ 0.7923	0.8468/ 0.7923	0.6846/ 0.7770

Otokodlayıcı + Pekiştirmeli Öğrenme Derin Q-Ağı	0.9948/ 0.6794	1.00/ 0.6987	0.9896 / 0.6794	0.9948/ 0.6758	0.9897 / 0.6553

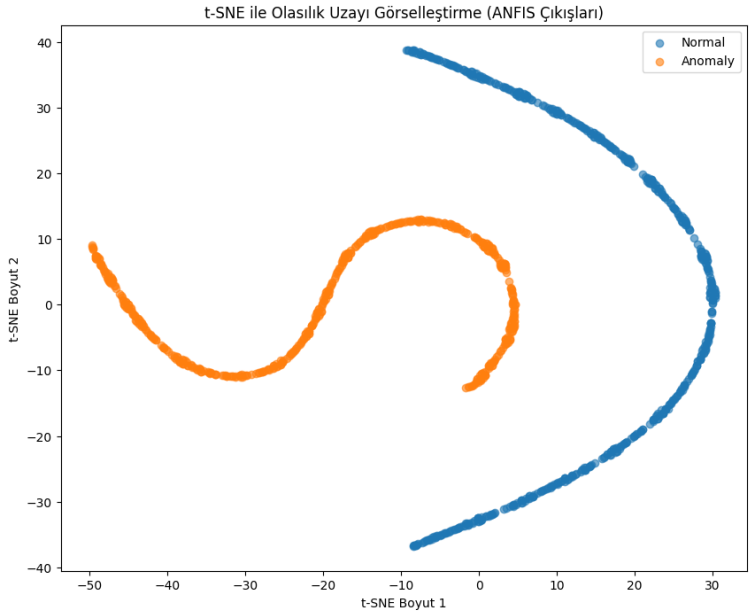
Edge-IIoTset veri seti üzerinde hibrit tabanlı yöntemlerin performansını değerlendirmek amacıyla Çizelge 4.28'de sunulan metrikler incelenmiştir. Bu çizelgede, ANFIS ve pekiştirmeli öğrenme yöntemlerinin ikili ve çoklu etiket sınıflandırmalarındaki performansları karşılaştırılmıştır. ANFIS yöntemi, ikili etiket sınıflandırmada 0.8191 isabetlilik, 0.7343 kesinlik ve 1.0000 duyarlılık ile dengesiz bir performans sergilerken, çoklu etiket sınıflandırmada 0.7923 isabetlilik, 0.8165 kesinlik ve 0.7770 MCC değerleriyle daha iyi sonuçlar elde etmiştir. pekiştirmeli öğrenme yöntemi ise ikili etiket sınıflandırmada 0.9948 isabetlilik, 1.0000 kesinlik ve 0.9897 MCC ile oldukça yüksek bir performans gösterirken, çoklu etiket sınıflandırmada 0.6794 isabetlilik, 0.6987 kesinlik ve 0.6553 MCC ile daha düşük bir başarı sergilemiştir. Bu sonuçlar, pekiştirmeli öğrenme yönteminin ikili sınıflandırmada üstün olduğunu, ancak çoklu etiket sınıflandırmada ANFIS daha iyi performans sunduğunu göstermektedir.

Çizelge 4.29. Edge-IIoTset Veri Seti Üzerinde Kullanılan ANFIS Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	Kesinlik	Duyarlılık	F-1 Skoru	Destek
İkili Etiket				
Normal	1.00	0.64	0.78	7491
Anomali	0.73	1.00	0.85	7491
Çoklu Etiket				
Backdoor	0.96	0.94	0.95	969
DDoS_HTTP	0.86	0.62	0.72	969
DDoS_ICMP	1.00	1.00	1.00	969
DDoS_TCP	1.00	0.57	0.73	969
DDoS_UDP	1.00	1.00	1.00	969

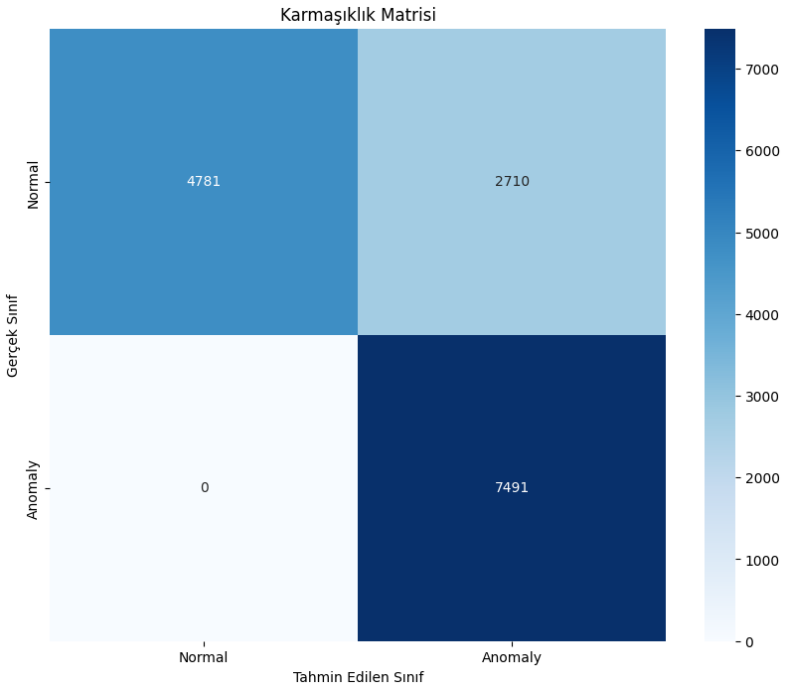
Normal	1.00	0.88	0.93	969
Password	0.49	0.49	0.49	969
Port_Scanning	0.68	1.00	0.81	969
Ransomware	0.88	0.97	0.92	969
SQL_injection	0.46	0.59	0.52	969
Uploading	0.71	0.52	0.60	969
Vulnerability_scanner	0.94	0.86	0.90	968
XSS	0.64	0.88	0.74	969

Çizelge 4.29, Edge-IIoTset veri seti üzerinde ANFIS algoritması ile elde edilen sınıflandırma performans metriklerini sınıflar bazında detaylandırmaktadır. İkili etiket sınıflandırmada, Normal sınıf için 1.0000 kesinlik ve 0.64 duyarlılık ile 0.78 F-1 skoru, Anomali sınıfında ise 0.73 kesinlik ve 1.0000 duyarlılık ile 0.85 F-1 skoru elde edilmiştir. Çoklu etiket sınıflandırmada, DDoS_ICMP ve DDoS_UDP sınıfları için kesinlik, duyarlılık ve F-1 skoru 1.0000 gibi mükemmel değerlere ulaşırken, Backdoor (0.95 F-1), Normal (0.93 F-1) ve Ransomware (0.92 F-1) sınıfları da yüksek performans göstermiştir. Ancak, Password (0.49 F-1) ve SQL_injection (0.52 F-1) sınıflarında düşük F-1 skorları dikkat çekmektedir. Bu sonuçlar, ANFIS yönteminin belirli anomali türlerinde (DDoS_ICMP ve DDoS_UDP) oldukça başarılı olduğunu, ancak Password ve SQL_injection sınıflarında performansın iyileştirilmeye ihtiyaç duyduğunu ortaya koymaktadır.



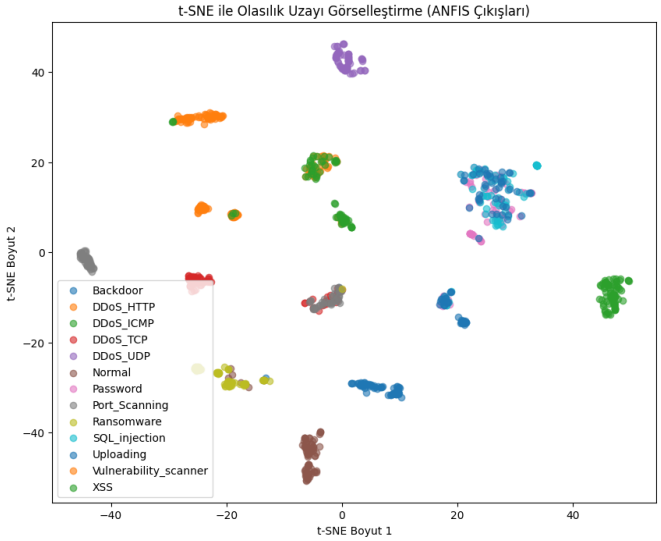
Şekil 4.53. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket t-SNE grafiği

Şekil 4.105, Edge-IIoTset veri seti üzerinde ANFIS yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasının t-SNE görselleştirmesini sunmaktadır. "Anomali" sınıfı dalgalı bir küme oluştururken, "Normal" sınıfı daha düzgün bir yay şeklinde dağılmaktadır. Bu ayrım, ANFIS yönteminin ikili sınıflandırma görevinde iki sınıfı birbirinden ayırt edebildiğini, ancak tam bir kümelenme başarısı sağlayamadığını göstermektedir.



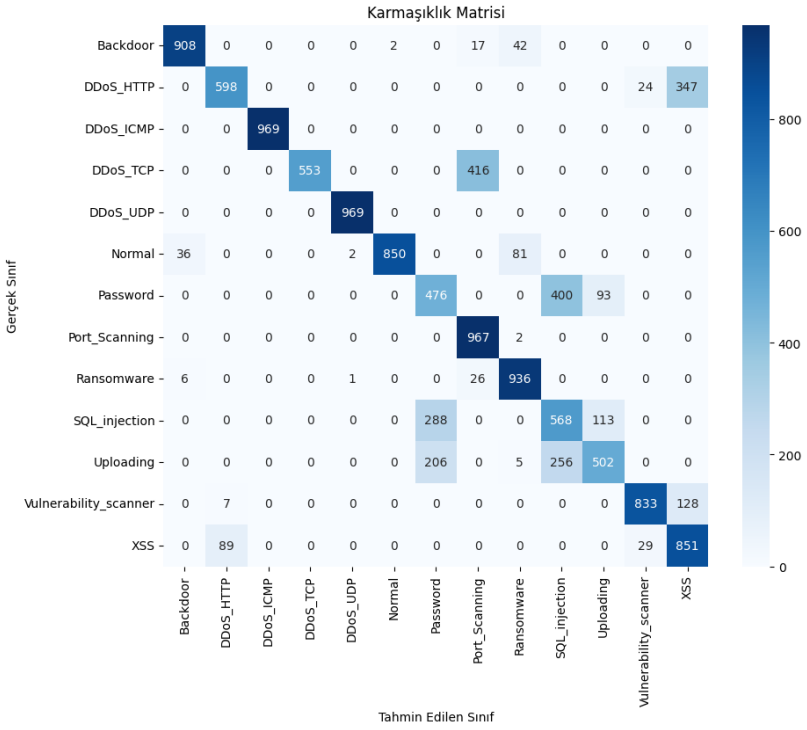
Şekil 4.54. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.54, Edge-IIoTset veri seti üzerinde ANFIS yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasının karmaşıklık matrisini yansıtmaktadır. "Normal" sınıfı için 4781 örnek doğru tahmin edilmiş, ancak 2710 örnek "Anomali" olarak yanlış sınıflandırılmıştır. "Anomali" sınıfı için 7491 örnek doğru tahmin edilirken, yanlış sınıflandırma bulunmamaktadır. Bu durum, ANFIS yönteminin "Anomali" sınıfını mükemmel bir doğrulukla ayırt edebildiğini, ancak "Normal" sınıfında önemli bir hata oranına sahip olduğunu göstermektedir.



Şekil 4.55. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket t-SNE grafiği

Şekil 4.55 üzerinden değerlendirildiğinde, ANFIS yöntemiyle gerçekleştirilen çoklu etiket sınıflandırmasının t-SNE görselleştirmesi, Backdoor, DDoS_HTTP, DDoS_ICMP, DDoS_TCP, DDoS_UDP, Normal, Password, Port_Scanning, Ransomware, SQL_Injection, Uploading ve XSS gibi sınıfların farklı bölgelerde kümelendiğini ortaya koymaktadır. Ancak, sınıflar arasında belirgin örtüşmeler dikkat çekmekte; örneğin, SQL_Injection ve Uploading gibi sınıflar daha dağınık bir yapı sergilerken, Backdoor ve DDoS_TCP gibi sınıflar nispeten daha kompakt kümeler oluşturmaktadır. Bu, ANFIS yönteminin çoklu etiket sınıflandırmasında ayrım gücünün sınırlı olduğunu ve benzer özelliklere sahip sınıflarda zorluk yaşadığını ifade etmektedir.



Şekil 4.56. Edge-IIoTset veri seti üzerinde uygulanan ANFIS yönteminin çoklu etiket karmaşıklık matrisi

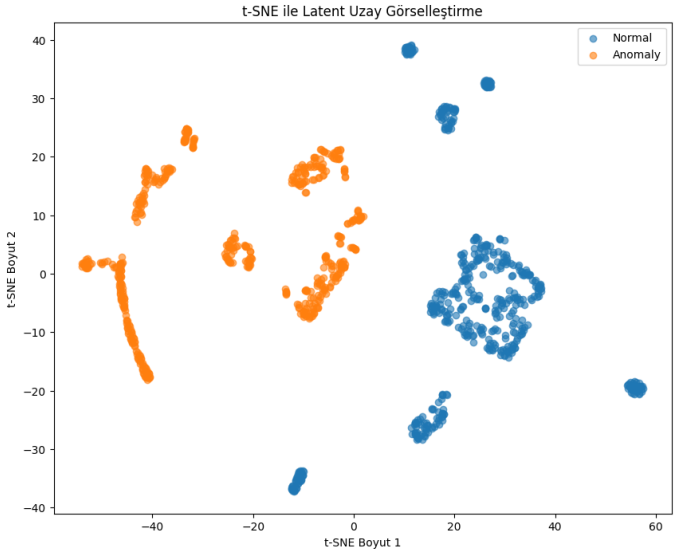
Şekil 4.56 üzerinden incelendiğinde, ANFIS yöntemiyle gerçekleştirilen çoklu etiket sınıflandırmasının karmaşıklık matrisi, XSS için 851, Backdoor için 908 doğru tahmini ortaya koymaktadır. Yanlış sınıflandırmalar arasında, XSS'nin 89 örneği Vulnerability_Scanner olarak yanlış tahmin edilmesi dikkat çekerken, SQL_Injection'da 568 doğru tahmine karşılık 113 örnek Uploading olarak yanlış sınıflandırılmıştır. Bu sonuçlar, ANFIS yönteminin çoklu etiket sınıflandırmasında genel olarak başarılı olduğunu, ancak bazı sınıflar arasında ayrım zorluğu yaşadığını ifade etmektedir.

Çizelge 4.30. Edge-IIoTset Veri Seti Üzerinde Kullanılan Pekiştirmeli Öğrenme Algoritması ile Elde Edilen Sınıflandırma Performans Metrikleri

Sınıf	Kesinlik	Duyarlılık	F-1 Skoru	Destek
İkili Etiket				
Normal	0.99	1.00	0.99	1638
Anomali	1.00	0.99	0.99	1638

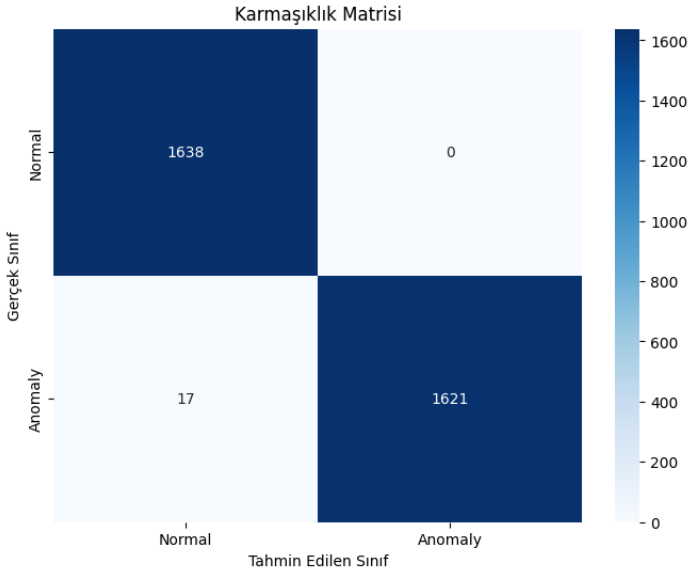
Çoklu Etiket				
Backdoor	0.63	0.44	0.52	969
DDoS_HTTP	0.86	0.62	0.72	969
DDoS_ICMP	0.98	1.00	0.99	969
DDoS_TCP	0.62	1.00	0.76	969
DDoS_UDP	0.99	1.00	1.00	969
Normal	0.64	0.62	0.63	969
Password	0.41	0.64	0.50	969
Port_Scanning	0.77	0.50	0.61	969
Ransomware	0.44	0.43	0.44	969
SQL_injection	0.49	0.42	0.45	969
Uploading	0.70	0.49	0.58	969
Vulnerability_scanner	0.90	0.85	0.87	968
XSS	0.63	0.83	0.71	969

Çizelge 4.30, Edge-IIoTset veri seti üzerinde pekiştirmeli öğrenme algoritması ile elde edilen sınıflandırma performans metriklerini sunmaktadır. İkili etiket sınıflandırmada, Normal sınıf için 0.99 kesinlik ve 1.0000 duyarlılık, Anomali sınıfında ise 1.0000 kesinlik ve 0.99 duyarlılık ile her iki sınıf için 0.99 F-1 skoru elde edilerek yüksek bir performans sergilenmiştir. Çoklu etiket sınıflandırmada, DDoS_ICMP (0.99 F-1) ve DDoS_UDP (1.0000 F-1) sınıfları yüksek başarı gösterirken, Vulnerability_scanner (0.87 F-1) ve DDoS_HTTP (0.72 F-1) sınıfları da kabul edilebilir sonuçlar vermiştir. Ancak, Ransomware (0.44 F-1), SQL_injection (0.45 F-1) ve Password (0.50 F-1) sınıflarında düşük F-1 skorları raporlanmıştır. Bu sonuçlar, pekiştirmeli öğrenme yönteminin ikili sınıflandırmada oldukça başarılı olduğunu, ancak çoklu etiket sınıflandırmada özellikle Ransomware, SQL_injection ve Password sınıflarında performansın geliştirilmesi gerektiğini göstermektedir.



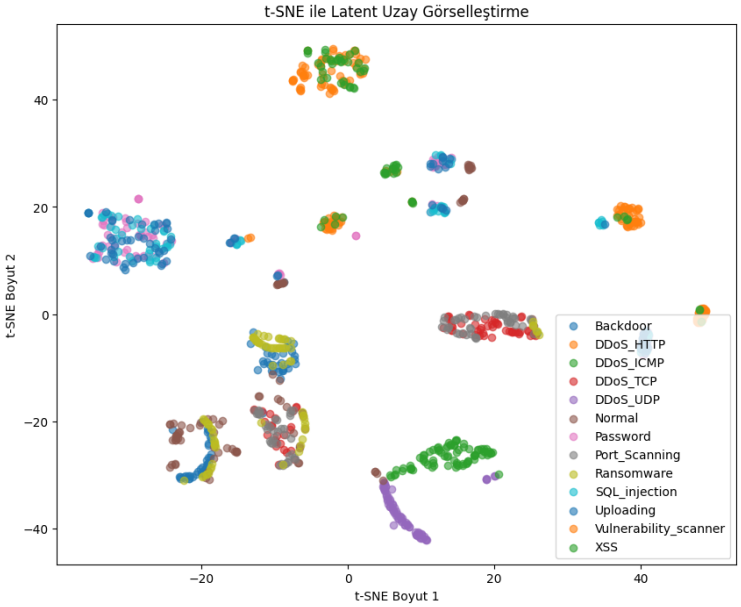
Şekil 4.57. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket t-SNE grafiği

Şekil 4.57, Edge-IIoTset veri seti üzerinde pekiştirmeli öğrenme yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasının t-SNE görselleştirmesini sunmaktadır. "Normal" sınıfı yoğun bir küme oluştururken, "Anomali" sınıfı daha dağınık ve birden fazla küme halinde dağılmaktadır. Bu ayrım, pekiştirmeli öğrenme yönteminin ikili sınıflandırma görevinde "Normal" sınıfını iyi bir şekilde tanımladığını, ancak "Anomali" sınıfında daha fazla çeşitlilik olduğunu göstermektedir.



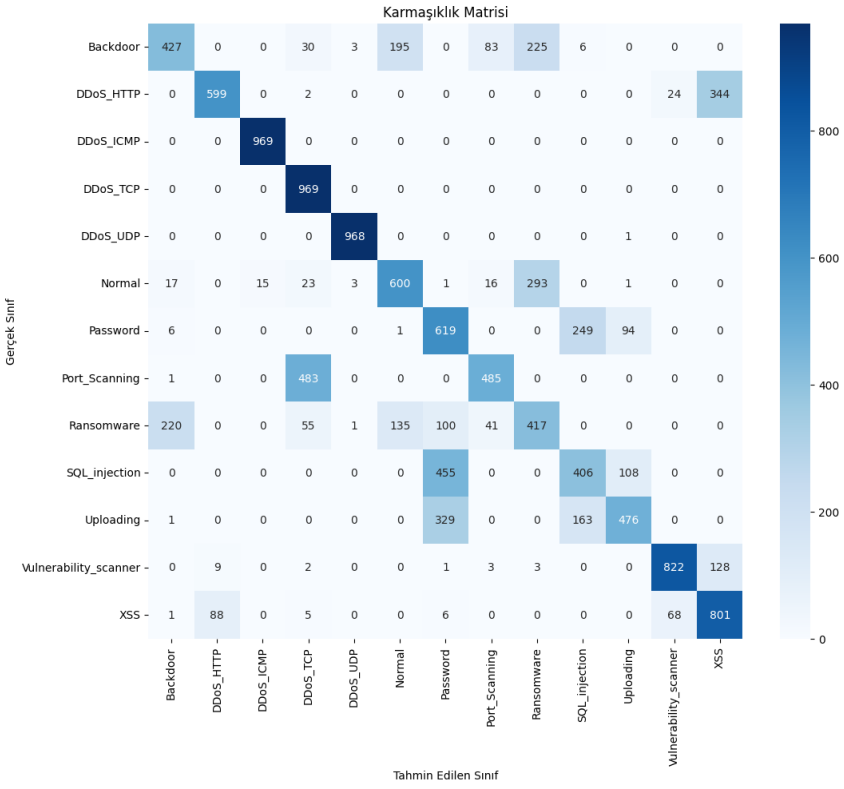
Şekil 4.58. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin ikili etiket karmaşıklık matrisi

Şekil 4.58, Edge-IIoTset veri seti üzerinde pekiştirmeli öğrenme yöntemiyle gerçekleştirilen ikili etiket sınıflandırmasının karmaşıklık matrisini ortaya koymaktadır. "Normal" sınıfı için 1638 örnek doğru tahmin edilmiş, ancak 17 örnek "Anomali" olarak yanlış sınıflandırılmıştır.



Şekil 4.59. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket t-SNE grafiği

Şekil 4.59 üzerinden değerlendirildiğinde, pekiştirmeli öğrenme yöntemiyle gerçekleştirilen çoklu etiket sınıflandırmasının t-SNE görselleştirmesi, Backdoor, DDoS_HTTP, DDoS_ICMP, DDoS_TCP, DDoS_UDP, Normal, Password, Port_Scanning, Ransomware, SQL_Injection, Uploading ve XSS gibi sınıfların farklı bölgelerde kümelendiğini ortaya koymaktadır. Sınıflar arasında bazı örtüşmeler olsa da, Backdoor ve XSS gibi sınıflar nispeten belirgin kümeler oluştururken, SQL_Injection ve Uploading daha dağınık bir dağılım sergilemektedir. Bu, yöntemin çoklu etiket ayrımında genel bir başarı sağladığını, ancak benzer özelliklere sahip sınıflarda zorluklar yaşadığını ifade etmektedir.



Şekil 4.60. Edge-IIoTset veri seti üzerinde uygulanan pekiştirmeli öğrenme yönteminin çoklu etiket karmaşıklık matrisi

Şekil 4.60 üzerinden incelendiğinde, pekiştirmeli öğrenme yöntemiyle gerçekleştirilen çoklu etiket sınıflandırmasının karmaşıklık matrisi, XSS için 801, Backdoor için 427 doğru tahmini sunmaktadır. Yanlış sınıflandırmalar arasında, XSS'nin 88 örneği Vulnerability_Scanner olarak yanlış tahmin edilmesi göze çarparken, SQL_Injection'da 406 doğru tahmine karşılık 108 örnek Uploading olarak yanlış

sınıflandırılmıştır. Bu, yöntemin çoklu etiket ayrımında genel bir başarı sergilediğini, ancak bazı sınıflar arasında karışıklık yaşadığını ifade etmektedir.

4.4. Elde Edilen Bulguların Karşılaştırılması

Çizelge 4.31, CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset veri setleri üzerinde çeşitli makine öğrenmesi modellerinin ikili ve çoklu etiket sınıflandırma görevlerindeki test isabetliliklerini sunmaktadır. Analiz, Fine Tree, Bagged Trees gibi klasik makine öğrenmesi modelleri, topluluk yöntemleri, CNN ve LSTM gibi derin öğrenme yaklaşımları ile ANFIS + GA ve Autoencoder + RL-DQN gibi hibrit yöntemleri kapsamaktadır. Bagged Trees, CIC-ToN-IoT veri setinde ikili sınıflandırmada %98,83, çoklu etiket sınıflandırmada %71,59; CSE-CIC-IDS2018 veri setinde ikili sınıflandırmada %96,94, çoklu etiket sınıflandırmada %94,28; Edge-IIoTset veri setinde ise ikili sınıflandırmada %100, çoklu etiket sınıflandırmada %92,12 isabetlilik elde etmiştir. Fine Tree, CIC-ToN-IoT veri setinde ikili sınıflandırmada %98,25, çoklu etiket sınıflandırmada %70,49; CSE-CIC-IDS2018'de %95,64/%91,11; Edge-IIoTset'te %100/%90,77 isabetlilik sağlamıştır. Medium Gaussian SVM, CIC-ToN-IoT veri setinde ikili sınıflandırmada %97,60, çoklu etiket sınıflandırmada %69,91; CSE-CIC-IDS2018'de %95,22/%91,16; Edge-IIoTset'te %100/%78,72 isabetlilik göstermiştir. ANFIS + GA, CIC-ToN-IoT veri setinde ikili sınıflandırmada %74,01, çoklu etiket sınıflandırmada %70,55; CSE-CIC-IDS2018'de %70,54/%91,45; Edge-IIoTset'te %81,91/%79,23 isabetlilik elde etmiştir. Boosted Trees, Edge-IIoTset veri setinde ikili sınıflandırmada %70,88, çoklu etiket sınıflandırmada %82,55; RUSBoosted Trees ise aynı veri setinde ikili sınıflandırmada %69,60, çoklu etiket sınıflandırmada %62,95 isabetlilik sağlamıştır. CNN, CIC-ToN-IoT veri setinde %97,92/%70,67, CSE-CIC-IDS2018'de %95,15/%91,46, Edge-IIoTset'te %100/%79,28 isabetlilik elde etmiştir. LSTM, CIC-ToN-IoT veri setinde %97,90/%70,99, CSE-CIC-IDS2018'de %95,02/%91,21, Edge-IIoTset'te %100/%79,73 isabetlilik göstermiştir. GA, CIC-ToN-IoT veri setinde %98,62/%71,72, CSE-CIC-IDS2018'de %95,70/%91,11, Edge-IIoTset'te %100/%89,92 isabetlilik sağlamıştır. Autoencoder + RL-DQN, CIC-ToN-IoT veri setinde %93,88/%68,17, CSE-CIC-IDS2018'de %93,22/%86,87, Edge-IIoTset'te %99,48/%67,94 isabetlilik elde etmiştir. Logistic Regression, CIC-ToN-IoT veri setinde

ikili sınıflandırmada %87,48, CSE-CIC-IDS2018'de %93,80, Edge-IIoTset'te %100 isabetlilik sağlamış, ancak çoklu etiket sınıflandırma sonuçları raporlanmamıştır.

Çizelge 4.31. Modellerin CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset Veri Setleri Üzerindeki Test İsabetlilik (%) Değerleri (İkili / Çoklu Etiket)

Model	**Hiperparametre Ayarları**	**CIC-ToN-IoT (İsabetlilik % (Test) : İkili Etiket / Çoklu Etiket)**	**CSE-CIC-IDS2018 (İsabetlilik % (Test) : İkili Etiket / Çoklu Etiket)**	**Edge-IIoTset (İsabetlilik % (Test) : İkili Etiket / Çoklu Etiket)**
Fine Tree	Maksimum bölünme sayısı: 100	98,25/70,49	95,64/91,11	100/90,77
Medium Tree	Maksimum bölünme sayısı: 20	96,05/64,07	94,33/78,22	100/63,23
Coarse Tree	Maksimum bölünme sayısı: 4	88,37/54,89	92,08/42,05	100/37,29
Linear Discriminant	Kovaryans yapısı: Full	83,74/58,82	93,22/85,41	99,95/50,89
Logistic Regression	-	87,48/-	93,80/-	100/-
Gaussian Naive Bayes	Dağılım: Gaussian	70,31/52,89	76,51/83,31	98,31/29,44

Medium Gaussian SVM	Çekirdek fonksiyonu: Gaussian	97,60/69,91	95,22/91,16	100/78,72
Fine KNN	Komşu sayısı: 1	97,54/63,12	94,87/89,42	100/77,86
Medium KNN	Komşu sayısı: 10	97,57/67,49	94,96/89,53	100/78,09
Coarse KNN	Komşu sayısı: 100	96,67/67,73	94,37/88,49	100/76,79
Cosine KNN	Komşu sayısı: 10	97,60/67,43	94,93/87,58	100/78,09
Weighted KNN	Komşu sayısı: 10	97,91/66,21	94,89/89,99	100/78,24
Boosted Trees	Topluluk yöntemi: AdaBoost	98,45/64,36	95,43/89,16	70,88/82,55
Bagged Trees	Topluluk yöntemi: Bag	98,83/71,59	96,94/94,28	100/92,12
Subspace Discriminant	Topluluk yöntemi: Subspace	82,92/57,41	92,60/79,74	100/54,83
RUSBoosted Trees	Topluluk yöntemi: RUSBoost	96,05/64,08	92,68/86,57	69,60/62,95
CNN	input_dim, num_classes, padding, batch_size=256, learning_rate=0.001, num_epochs=50, patience=5, dropout_rate=0.5, optimizer=Adam, criterion=CrossEntropyLoss, class_weights, device=cuda	97,92/70,67	95,15/91,46	100/79,28
LSTM	hidden_dim=128, num_layers=2, dropout=0.5, optimizer=Adam,	97,90/70,99	95,02/91,21	100/79,73

	lr=0.001, batch_size=256, epochs=50			
GA	Population=50, Generations=20, Crossover=0.7 (TwoPoint), Mutation=0.2 (FlipBit, indpb=0.03), Selection=NSGA-II, Fitness=(accuracy↑, f1-score↑, feature count↓), Classifier=RandomForest(n_estimators=30, max_depth=5)	98,62/71,72	95,70/91,11	100/89,92
ANFIS + GA	num_rules=30, mf_class=Gaussian, vanishing_strategy=blend, act_output=None, reg_lambda=0.01, optim=BaseGA, optim_params={'epoch': 50, 'pop_size': 50}, obj_name=F1S, seed=42, verbose=True, lb=(-1.0,), ub=(1.0,), mode=single, n_workers=None, termination=None	74,01/70,55	70,54/91,45	81,91/79,23
Autoencoder + RL-DQN	learning_rate=1e-4, buffer_size=100000, batch_size=128, gamma=0.99, exploration_initial_eps=1.0, exploration_final_eps=0.01, exploration_fraction=0.3, target_update_interval=500, train_freq=4, gradient_steps=4, verbose=1, tensorboard_log="./rl_log/"	93,88/68,17	93,22/86,87	99,48/67,94

BÖLÜM 5

TARTIŞMA

Bu çalışmada, siber-fiziksel sistemler ve endüstriyel kontrol sistemlerinde davetsiz misafir saldırılarının anomali tespiti için çeşitli yapay zeka ve yumuşak hesaplama yöntemleri sistematik bir şekilde incelenmiştir. CIC-ToN-IoT, CSE-CIC-IDS2018 ve Edge-IIoTset veri setleri üzerinde makine öğrenmesi (Bagged Trees, SVM, KNN gibi), derin öğrenme (CNN, LSTM), yumuşak hesaplama (GA) ve hibrit (ANFIS, DQN) teknikleri kullanılarak modeller geliştirilmiştir. Öncelikle literatür taraması yapılarak kullanılan yöntemlerin teorik temelleri ile bu yöntemlerin daha önceki çalışmalardaki uygulamaları incelenmiştir. Ardından, uygun veri setleri hazırlanarak bu yöntemlere dayalı matematiksel modeller oluşturulmuştur. Bu modellerin performansı, ikili ve çoklu etiket sınıflandırma görevlerinde test edilerek, isabetlilik ve F1-skoru gibi metriklerle değerlendirilmiştir. Çalışma, bu yöntemlerin siber güvenlik bağlamındaki uygulanabilirliğini ortaya koymayı amaçlamıştır.

Modellerin performansı, veri setinin yapısına ve sınıflandırma görevine bağlı olarak önemli farklılıklar göstermiştir. Çizelge 4.31, ikili ve çoklu etiket sınıflandırma görevlerindeki test isabetliliklerini özetlemekte olup, F1-skorları gibi diğer metrikler sonuçlar bölümünde ayrıntılı bir şekilde sunulmuştur. Bagged Trees, CIC-ToN-IoT veri setinde ikili sınıflandırmada %98,83, çoklu etiket sınıflandırmada %71,59; Edge-IIoTset veri setinde ikili sınıflandırmada %100, çoklu etiket sınıflandırmada %92,12 isabetlilik elde ederek, topluluk tabanlı yöntemlerin farklı veri setlerinde tutarlı bir genelleme yeteneği sunduğunu göstermiştir. Ancak, Edge-IIoTset'te birçok modelin ikili sınıflandırmada %100'e yakın isabetlilik sağlamasına rağmen, çoklu etiket

sınıflandırmada performansın düşmesi (örneğin, Fine Tree: %100/%90,77; CNN: %100/%79,28), saldırı türlerini ayırt etmenin normal/saldırı ayrımından daha karmaşık olduğunu ortaya koymaktadır. Bu, çoklu etiket sınıflandırmada sınıf ayrılabilirliğinin ve öznitelik ilişkilerinin kritik bir rol oynadığını düşündürmektedir.

Klasik makine öğrenmesi modelleri, hibrit yöntemlere kıyasla genellikle daha yüksek isabetlilik sunmuştur. Fine Tree, CIC-ToN-IoT veri setinde ikili sınıflandırmada %98,25, çoklu etiket sınıflandırmada %70,49; Edge-IIoTset'te %100/%90,77 isabetlilik elde etmiştir. Medium Gaussian SVM de benzer şekilde CIC-ToN-IoT'ta %97,60/%69,91, Edge-IIoTset'te %100/%78,72 isabetlilik sağlamıştır. Buna karşılık, ANFIS + GA gibi hibrit yöntemler CIC-ToN-IoT'ta ikili sınıflandırmada %74,01, çoklu etiket sınıflandırmada %70,55; Edge-IIoTset'te %81,91/%79,23 isabetlilikle daha düşük ve dengesiz performans göstermiştir. Örneğin, ANFIS, "XSS" sınıfında %100 F-1 skoruyla başarılı olurken, "Password" sınıfında %29-%49 F-1 ile zorlanmıştır. Bu, hibrit modellerin karmaşık yapısının, özellikle öznitelik açısından zengin veri setlerinde genelleme kabiliyetini sınırlayabileceğini işaret etmektedir. Edge-IIoTset'te Boosted Trees (%70,88) ve RUSBoosted Trees (%69,60) gibi topluluk modellerinin düşük performansı, veri setinin öznitelik yapısının bu modellerle uyumsuz olabileceğini göstermektedir.

CSE-CIC-IDS2018 veri setinde, Bagged Trees ikili sınıflandırmada %96,94, çoklu etiket sınıflandırmada %94,28 isabetlilikle dengeli bir performans sergilemiştir. CNN (%95,15/%91,46) ve LSTM (%95,02/%91,21) modelleri tutarlı sonuçlar vermiş; "Bot" ve "DDoS-HOIC" gibi sınıflarda %100 F-1 skoruyla başarılı olunurken, "Infiltration" sınıfında %61-%73 F-1 ile sınırlı performans gözlenmiştir. GA, %95,70 ikili ve %91,11 çoklu etiket isabetliliğiyle yüksek kesinlik (%98,70) sunmuş, ancak "Infiltration" sınıfında %68 F-1 ile zorlanmıştır. Pekiştirmeli öğrenme, %93,22 ikili ve %86,51 çoklu etiket F-1 skoruyla dengeli bir performans göstermiş, ancak "Infiltration" sınıfında %61 F-1 ile zayıf kalmıştır. Lojistik Regresyon, temel yapısı gereği çoklu etiketli sınıflandırma için uygun olmadığından bu görevde değerlendirilmemiştir. Ancak ikili sınıflandırma senaryolarında (örneğin, Edge-IIoTset: %100 doğruluk) oldukça güçlü sonuçlar vermiştir. Bu durum, modelin tasarımına uygun olup bir eksiklik olarak değerlendirilmemiştir.

Hiperparametre ayarlarının performansa etkisi önemli bir bulgudur. Karar ağaçlarında maksimum bölünme sayısının artırılması (Fine Tree: 100 bölünme; Coarse Tree: 4 bölünme), isabetliliği iyileştirmiştir; örneğin, Coarse Tree Edge-IIoTset'te %100/%37,29 isabetlilikle sınırlı kalırken, Fine Tree %100/%90,77 sağlamıştır. KNN modellerinde komşu sayısının artırılması (Fine KNN: 1 komşu; Coarse KNN: 100 komşu), çoklu etiket sınıflandırmada genelleme yeteneğini artırmıştır. Derin öğrenme modelleri (CNN: %97,92/%70,67; LSTM: %97,90/%70,99), klasik modellere yakın performans gösterse de, yüksek hesaplama maliyeti nedeniyle ek yük getirmiştir. Sınıf bazlı performanslar incelendiğinde, "Backdoor" (%100 F-1) ve "DDoS_ICMP" (%100 F-1) gibi sınıflarda modellerin mükemmel sonuçlar verdiği, ancak "Injection" (%27-%28 F-1) ve "Password" (%29-%49 F-1) gibi azınlık sınıflarında düşük performans gösterdiği gözlenmiştir. Bu, sınıf dengesizliğinin veya azınlık sınıflarının karmaşıklığının modellerin performansını etkilediğini düşündürmektedir.

Edge-IIoTset veri setinde çok sayıda modelin ikili sınıflandırmada %100 isabetlilik elde etmesi, veri setinin 30 öznitelik ve 13 dengeli sınıf içeren yapısının, normal ve saldırı trafiğini ayırmada yüksek ayırt edicilik sunduğunu göstermektedir. Çizelge 4.21'de belirtilen "http.request.method" ve "tcp.flags" gibi öznitelikler, bu yüksek performansı desteklemiş olabilir. Buna karşılık, CIC-ToN-IoT (40 öznitelik, 6 sınıf) ve CSE-CIC-IDS2018 (36 öznitelik, 11 sınıf) veri setlerinde karmaşık öznitelik ilişkileri ve artan sınıf sayısı, isabetliliği düşürmüştür. Örneğin, Fine Tree'nin CIC-ToN-IoT'ta %98,25, CSE-CIC-IDS2018'de %95,64 isabetlilik sağlaması, Edge-IIoTset'teki %100 isabetliliğe kıyasla daha karmaşık bir problem uzayına işaret etmektedir. Fine Tree ve Coarse Tree gibi modellerin Edge-IIoTset'te benzer isabetlilikler sağlaması, yüksek performansın model karmaşıklığından ziyade veri setinin yapısına bağlı olduğunu göstermektedir.

Bu çalışma, siber-fiziksel sistemlerde izinsiz giriş ve ağ anomalisi tespiti için geliştirilen modellerin, veri setinin yapısı, sınıf dengesi ve hesaplama maliyeti gibi faktörlere bağlı olarak farklı performanslar sergilediğini göstermiştir. Gelecekte, bu modellerin IoT cihazları, otonom araçlar, endüstriyel otomasyon sistemleri, akıllı şebekeler ve ağ altyapıları (örneğin, switch ve router'lar) gibi geniş bir yelpazedeki siber-fiziksel sistemlerde gerçek zamanlı uygulanabilirliği araştırılabilir. Örneğin, Bagged Trees ve Fine Tree gibi klasik makine öğrenmesi modelleri, yüksek isabetlilikleri

(örneğin, Edge-IIoTset'te %100 ikili sınıflandırma) ve düşük hesaplama maliyetleri nedeniyle, kaynak kısıtlı IoT cihazları veya yüksek hızlı veri akışına sahip ağ cihazlarında ağ anomalisi tespiti için etkili bir şekilde kullanılabilir. Ancak, bu modellerin yorumlanabilirlik açısından sınırlı olması, özellikle otonom araçlar veya endüstriyel kontrol sistemleri gibi güvenlik açısından kritik uygulamalarda, model kararlarının açıklanmasını zorlaştırabilir. Buna karşılık, ANFIS ve GA gibi yumuşak hesaplama yöntemleri, daha yüksek yorumlanabilirlik sunarak, sistem operatörlerinin saldırı türlerini (örneğin, DDoS, Injection) ve model kararlarını daha iyi anlamasını sağlayabilir. Bu avantaj, özellikle azınlık sınıflarında düşük performans gösteren bu yöntemlerin (örneğin, "Injection": %27 F-1; "Password": %29-%49 F-1), sınıf ağırlıklandırma, sentetik veri üretimi veya transfer öğrenme gibi tekniklerle optimize edilmesi durumunda, akıllı şebekeler veya endüstriyel otomasyon sistemlerinde ağ güvenliği uygulamalarını güçlendirebilir. Pekiştirmeli öğrenme, dinamik ortamlara uyum sağlama potansiyeliyle (örneğin, Edge-IIoTset: %99,48 ikili sınıflandırma) dikkat çekse de, yüksek hesaplama maliyeti, kaynak kısıtlı cihazlarda uygulanmasını sınırlayabilir. Gelecek çalışmalar, klasik makine öğrenmesi ile yumuşak hesaplama yöntemlerinin hibrit yaklaşımlarını geliştirerek, hem yüksek performans hem de yorumlanabilirlik sunan çözümler üretebilir. Örneğin, akıllı şebeke ortamlarında, ağ tabanlı izinsiz giriş tespiti için modellerin simülasyonlar aracılığıyla test edilmesi, gerçek zamanlı performanslarını değerlendirmek adına değerli olabilir. Bu tür çalışmalar, sınıf dengesizliği sorununu ele almak için yeni veri ön işleme teknikleri veya özelleştirilmiş model mimarileri geliştirilmesine odaklanabilir, böylece siber-fiziksel ve endüstriyel kontrol sistemlerinde daha güvenilir ve uyarlanabilir anomali tespiti çözümleri sunulabilir.

KAYNAKLAR

Abshari, D., & Sridhar, M. (2025). A Survey of Anomaly Detection in Cyber-Physical Systems (arXiv:2502.13256). arXiv. https://doi.org/10.48550/arXiv.2502.13256

Adjei, P. O., Tetarave, S. K., John, C., Manneh, M., & Pattnayak, P. (2024). Robust Network Anomaly Detection with K-Nearest Neighbors (KNN) Enhanced Digital Twins. SoutheastCon 2024, 421–426. https://doi.org/10.1109/SoutheastCon52093.2024.10500053

Agrawal, N., & Kumar, R. (2022). Security Perspective Analysis of Industrial Cyber Physical Systems (I-CPS): A Decade-wide Survey. ISA Transactions, 130, 10–24. https://doi.org/10.1016/j.isatra.2022.03.018

Alcaraz, C., & Lopez, J. (2022). Digital Twin: A Comprehensive Survey of Security Threats. IEEE Communications Surveys & Tutorials, 24(3), 1475–1503. https://doi.org/10.1109/COMST.2022.3171465

Alem, S., Espes, D., Nana, L., Martin, E., & De Lamotte, F. (2023). A novel bi-anomaly-based intrusion detection system approach for industry 4.0. Future Generation Computer Systems, 145, 267–283. https://doi.org/10.1016/j.future.2023.03.024

Al-Fuhaidi, B., Farae, Z., Al-Fahaidy, F., Nagi, G., Ghallab, A., & Alameri, A. (2024). Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms. Applied Computational Intelligence and Soft Computing, 2024(1), 2625922. https://doi.org/10.1155/2024/2625922

Aliev, R. A., Pedrycz, W., Huseynov, O., Aliyev, R., & GUIRIMOV, B. G. (2024). Approximate Reasoning Based on Similarity of Z-numbers. Iranian Journal of Fuzzy Systems, 21(1). https://doi.org/10.22111/ijfs.2024.46303.8170

Anoop V.S., Verma, S., & Govindarajan, U. H. (2025). Advances in Artificial Intelligence for Healthcare Applications (1st ed.). CRC Press. https://doi.org/10.1201/9781003503385

Applied Computational Intelligence and Soft Computing, 2024(1), 2625922. https://doi.org/10.1155/2024/2625922

Aronson, J. E. (2003). Expert Systems. In *Encyclopedia of Information Systems* (pp. 277-289). Elsevier. https://doi.org/10.1016/B0-12-227240-4/00067-8

Azad, M., Chikalov, I., Hussain, S., Moshkov, M., & Zielosko, B. (2022). Decision Trees with Hypotheses. Springer International Publishing. https://doi.org/10.1007/978-3-031-08585-7

Azimjonov, J., & Kim, T. (2024). Stochastic gradient descent classifier-based lightweight intrusion detection systems using the efficient feature subsets of datasets. Expert Systems with Applications, 237, 121493. https://doi.org/10.1016/j.eswa.2023.121493

Baybulatov, A. A., & Promyslov, V. G. (2021). Industrial Control System Availability Assessment with a Metric Based on Delay and Dependency. IFAC-PapersOnLine, 54(13), 472–476. https://doi.org/10.1016/j.ifacol.2021.10.493

Bhatia, M. P. S., & Sangwan, S. R. (2024). Soft computing for anomaly detection and prediction to mitigate IoT-based real-time abuse. Personal and Ubiquitous Computing, 28(1), 123–133. https://doi.org/10.1007/s00779-021-01567-8

Bicaku, A., Schmittner, C., Rottmann, P., Tauber, M., & Delsing, J. (2019). Security Safety and Organizational Standard Compliance in Cyber Physical Systems. Infocommunications Journal, 1, 2–9. https://doi.org/10.36244/ICJ.2019.1.1

Catillo, M., Pecchia, A., & Villano, U. (2023). CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders. Computers & Security, 129, 103210. https://doi.org/10.1016/j.cose.2023.103210

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Datta Gupta, K., Singhal, K., Sharma, D. K., Sharma, N., & Malebary, S. (2023). Fuzzy Controller-empowered Autoencoder Framework for anomaly detection in Cyber Physical Systems. Computers and Electrical Engineering, 108, 108685. https://doi.org/10.1016/j.compeleceng.2023.108685

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors, 24(4), 1328. https://doi.org/10.3390/s24041328

Dix, A. (2025). *Artificial Intelligence: Humans at the Heart of Algorithms* (2nd ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003082880

Duo, W., Zhou, M., & Abusorrah, A. (2022). A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica, 9(5), 784–800. https://doi.org/10.1109/JAS.2022.105548

El-Kady, A. H., Halim, S., El-Halwagi, M. M., & Khan, F. (2023). Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Safety and Environmental Protection, 173, 384–413. https://doi.org/10.1016/j.psep.2023.03.012

Faisal, A., Al-Nahhal, I., Dobre, O. A., & Ngatched, T. M. N. (2024). Reinforcement Learning for Reconfigurable Intelligent Surfaces: Assisted Wireless Communication Systems. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-52554-4

Falcone, R., Lima, C., & Martinelli, E. (2020). Soft computing techniques in structural and earthquake engineering: A literature review. *Engineering Structures*, *207*, 110269. https://doi.org/10.1016/j.engstruct.2020.110269

Feng, X., & Hu, S. (2023). Cyber-Physical Zero Trust Architecture for Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Cyber-Physical Systems, 1, 394–405. https://doi.org/10.1109/TICPS.2023.3333850

Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access, 10, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809

Ganesan, P., & Arockia Edwin Xavier, S. (2023). An Intelligent Intrusion Detection System in Smart Grid Using PRNN Classifier. Intelligent Automation & Soft Computing, 35(3), 2979–2996. https://doi.org/10.32604/iasc.2023.029264

Guato Burgos, M. F., Morato, J., & Vizcaino Imacaña, F. P. (2024). A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence. Applied Sciences, 14(3), 1194. https://doi.org/10.3390/app14031194

Hagenaars, J. A., Kühnel, S., & Andreß, H.-J. (2025). Interpreting and comparing effects in logistic, probit, and logit regression. Sage.

He, Y., & Shen, W. (2025). Agent-based digital twins for collaborative machine intelligence solutions. IET Collaborative Intelligent Manufacturing, 7(1), e70018. https://doi.org/10.1049/cim2.70018

Hewapathirana, I. U. (2025). A Comparative Study of Two-Stage Intrusion Detection Using Modern Machine Learning Approaches on the CSE-CIC-IDS2018 Dataset. Knowledge, 5(1), 6. https://doi.org/10.3390/knowledge5010006

Hoshino, Y., Rathnayake, N., Linh Dang, T., & Rathnayake, U. (2024). Cascaded-ANFIS and Its Successful Real-World Applications. In P. Balasubramaniam & N. Ramesh Babu (Eds.), Fuzzy Logic Controllers and Applications. IntechOpen. https://doi.org/10.5772/intechopen.1006491

Hua, P. (2024). Neural Networks with TensorFlow and Keras: Training, Generative Models, and Reinforcement Learning. Apress. https://doi.org/10.1007/979-8-8688-1020-6

Huang, X., Liu, J., Lai, Y., Mao, B., & Lyu, H. (2023). EEFED: Personalized Federated Learning of Execution&Evaluation Dual Network for CPS Intrusion Detection. IEEE Transactions on Information Forensics and Security, 18, 41–56. https://doi.org/10.1109/TIFS.2022.3214723

Ishwaran, H. (2025). Multivariate Statistics: Classical Foundations and ModernMachine Learning (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003493679

ISO/IEC. (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO/IEC 27005:2022). International Organization for Standardization. https://www.iso.org/standard/80585.html

Jan, M. A., Khan, F., Khan, R., Mastorakis, S., Menon, V. G., Alazab, M., & Watters, P. (2021). Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS. IEEE Transactions on Industrial Informatics, 17(8), 5829–5839. https://doi.org/10.1109/TII.2020.3043802

Javaheri, D., Gorgin, S., Lee, J.-A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. Information Sciences, 626, 315–338. https://doi.org/10.1016/j.ins.2023.01.067

Jeffrey, N., Tan, Q., & Villar, J. R. (2024). A hybrid methodology for anomaly detection in Cyber–Physical Systems. Neurocomputing, 568, 127068. https://doi.org/10.1016/j.neucom.2023.127068

Jentzen, A., Kuckuck, B., & Wurstemberger, P. von. (2025). Mathematical Introduction to Deep Learning: Methods, Implementations, and Theory (arXiv:2310.20360). arXiv. https://doi.org/10.48550/arXiv.2310.20360

Jurafsky, D., & Martin, J. H. (2025). Speech and language processing: An introduction to natural language processing, computational linguistics, and speech recognition with language models (3rd ed.) [Online manuscript]. https://web.stanford.edu/~jurafsky/slp3/

Kanagachidambaresan, G. R., & Bharathi, N. (2024). Learning Algorithms for Internet of Things: Applying Python Tools to Improve Data Collection Use for System Performance. Apress. https://doi.org/10.1007/979-8-8688-0530-1

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kavallieratos, G., Grigoriadis, C., Katsika, A., Spathoulas, G., Kotzanikolaou, P., & Katsikas, S. (2022). Risk assessment and control selection for cyber-physical

systems: A case study on supply chain tracking systems. Journal of Surveillance, Security and Safety, 3(4), 128–149. https://doi.org/10.20517/jsss.2022.17

Kaveh, A., & Yousefpoor, H. (2024). Chaotic Meta-heuristic Algorithms for Optimal Design of Structures (Vol. 1129). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-48918-1

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of Industrial Cyber-Physical Systems: A Review. ACM Computing Surveys, 54(11s), 1–35. https://doi.org/10.1145/3510410

Khalil, S. M., Bahsi, H., Dola, H. O., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber-Physical Systems—A Case Study of a Microgrid System. Computers & Security, 124, 102950. https://doi.org/10.1016/j.cose.2022.102950

Khilar, R., Mariyappan, K., Christo, M. S., Amutharaj, J., Anitha, T., Rajendran, T., & Batu, A. (2022). Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things. Wireless Communications and Mobile Computing, 2022, 1–10. https://doi.org/10.1155/2022/1440538

Kroese, D. P., Botev, Z. I., Taimre, T., & Vaisman, R. (2020). Data science and machine learning: Mathematical and statistical methods. CRC Press, Taylor & Francis Group.

Kumar, A., Rathore, P. S., Ahuja, S., & Lilhore, U. K. (Eds.). (2025). Front Matter. In Integrating Neurocomputing with Artificial Intelligence (1st ed.). Wiley. https://doi.org/10.1002/9781394335718.fmatter

Kumar, T. A., Julie, E. G., Burugadda, V. R., Kumar, A., & Kumar, P. (Eds.). (2024). Front Matter. In Computational Intelligence (1st ed.). Wiley. https://doi.org/10.1002/9781394214259.fmatter

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. Computers, 14(2), 49. https://doi.org/10.3390/computers14020049

Lanham, M. (2023). Evolutionary deep learning: Genetic algorithms and neural networks. Manning.

Lapan, M. (2024). Deep reinforcement learning hands-on: A practical and easy-to-follow guide to RL from Q-learning and DQNs to PPO and RLHF, third edition (3rd ed). Packt Publishing.

Leander, B., Čaušević, A., & Hansson, H. (2019). Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. Proceedings of the 14th International Conference on Availability, Reliability and Security, 1–8. https://doi.org/10.1145/3339252.3341481

Li, Y., Gu, W., Yuan, M., & Tang, Y. (2022). Real-time data-driven dynamic scheduling for flexible job shop with insufficient transportation resources using hybrid deep Q network. Robotics and Computer-Integrated Manufacturing, 74, 102283. https://doi.org/10.1016/j.rcim.2021.102283

Liu, W., Zhang, Z., Qiao, X., Li, Y., Tan, Y., & Meng, W. (2024). A Software Integrity Authentication Protocol for Zero Trust Architecture. Proceedings of the SIGCOMM Workshop on Zero Trust Architecture for Next Generation Communications, 1–6. https://doi.org/10.1145/3672200.3673874

Liu, X., Shuang, N., Saklain, M. G., Huang, H., Zhang, L., & Deng, F. (2024). A Network Intrusion Detection Method for Training Dataset Generation Based on KNN. Proceedings of the International Conference on Image Processing, Machine Learning and Pattern Recognition, 231–236. https://doi.org/10.1145/3700906.3700944

Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. SECURITY AND PRIVACY, 6(6), e318. https://doi.org/10.1002/spy2.318

Mansour, R. F. (2022). Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment. Scientific Reports, 12(1), 12937. https://doi.org/10.1038/s41598-022-17043-z

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems, 133, 95–113. https://doi.org/10.1016/j.future.2022.03.001

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems, 133, 95–113. https://doi.org/10.1016/j.future.2022.03.001

Maseno, E. M., Wang, Z., & Xing, H. (2022). A Systematic Review on Hybrid Intrusion Detection System. Security and Communication Networks, 2022, 1–23. https://doi.org/10.1155/2022/9663052

Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. International Journal of Critical Infrastructure Protection, 35, 100464. https://doi.org/10.1016/j.ijcip.2021.100464

Mitchell, M. (1996). An introduction to genetic algorithms. MIT Press.

N. V. Jagan Mohan, R., Chandra Sekhar, V., & M. N. S. S. V. K. R. Gupta, V. (2024). Algorithms in Advanced Artificial Intelligence: ICAAAI-2023 (1st ed.). CRC Press. https://doi.org/10.1201/9781003529231

Oks, S. J., Jalowski, M., Lechner, M., Mirschberger, S., Merklein, M., Vogel-Heuser, B., & Möslein, K. M. (2024). Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. Information Systems Frontiers, 26(5), 1731–1772. https://doi.org/10.1007/s10796-022-10252-x

Pradhan, M. (2023). Information and Knowledge Systems (1st ed). Nova Science Publishers, Incorporated.

Putnik, G., Ferreira, L., Lopes, N., & Putnik, Z. (2019). What is a Cyber-Physical System: Definitions and models spectrum. FME Transactions, 47(4), 663–674. https://doi.org/10.5937/fmet1904663P

Raman, M. R. G., & Mathur, A. P. (2022). A Hybrid Physics-Based Data-Driven Framework for Anomaly Detection in Industrial Control Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(9), 6003–6014. https://doi.org/10.1109/TSMC.2021.3131662

Rizzardi, A., Sicari, S., & Coen-Porisini, A. (2022). Analysis on functionalities and security features of Internet of Things related protocols. Wireless Networks, 28(7), 2857–2887. https://doi.org/10.1007/s11276-022-02999-7

Rudas, I. J. (2003). Hybrid Systems. In *Encyclopedia of Information Systems* (pp. 563–570). Elsevier. https://doi.org/10.1016/B0-12-227240-4/00088-5

Saheed, Y. K., Abdulganiyu, O. H., Majikumna, K. U., Mustapha, M., & Workneh, A. D. (2024). ResNet50-1D-CNN: A new lightweight resNet50-One-dimensional convolution neural network transfer learning-based approach for improved intrusion detection in cyber-physical systems. International Journal of Critical Infrastructure Protection, 45, 100674. https://doi.org/10.1016/j.ijcip.2024.100674

Sajid, M., Kumar Sagar, A., Singh, J., Khalaf, O. I., & Prasad, M. (2023). Intelligent Techniques for Cyber-Physical Systems (1st ed.). CRC Press. https://doi.org/10.1201/9781003438588

Salerno, S. (2025). Tiny Machine Learning Quickstart: Machine Learning for Arduino Microcontrollers. Apress. https://doi.org/10.1007/979-8-8688-1294-1

Sarhan, M., Layeghy, S., & Portmann, M. (2022). Evaluating Standard Feature Sets Towards Increased Generalisability and Explainability of ML-based Network Intrusion Detection. Big Data Research, 30, 100359. https://doi.org/10.1016/j.bdr.2022.100359

Saßnick, O., Rosenstatter, T., Schäfer, C., & Huber, S. (2024). STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review. *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*, 1–8. https://doi.org/10.1109/ICPS59941.2024.10639949

Sharma, A., Rani, S., Shah, S. H., Sharma, R., Yu, F., & Hassan, M. M. (2023). An Efficient Hybrid Deep Learning Model for Denial of Service Detection in Cyber Physical Systems. IEEE Transactions on Network Science and Engineering, 10(5), 2419–2428. https://doi.org/10.1109/TNSE.2023.3273301

Shivam, Midha, S., & Ramola, B. (2022). Cryptography in Network Security. 2022 International Conference on Cyber Resilience (ICCR), 1–5. https://doi.org/10.1109/ICCR56254.2022.9996070

Siddique, N., & Adeli, H. (2013). Computational intelligence: Synergies of fuzzy logic, neural networks, and evolutionary computing. John Wiley & Sons Inc. https://doi.org/10.1002/9781118534823

Siddique, N., Arefin, M. S., Kaiser, M. S., & Kayes, A. (2023). Applied Intelligence for Industry 4.0 (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003256083

Singh, M., & Chauhan, N. (2024). Convolutional Neural Network Based IOT Intrusion Detection System using Edge-IIoTset. 2024 International Conference on Integrated Circuits, Communication, and Computing Systems (ICIC3S), 1–4. https://doi.org/10.1109/ICIC3S61846.2024.10603309

Sood, V. K., Murari, K., Gupta, O. H., & Kumar, A. (2024). Soft Computing Applications for Advancements in Power Systems (1st ed.). River Publishers. https://doi.org/10.1201/9788770046862

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) security (NIST SP 800-82r3; p. NIST SP 800-82r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-82r3

Tabakov, I. G. (with Politechnika Wrocławska). (2022). Discrete mathematical structures. Pt. 2: Algebraic systems. WUST Publishing House.

Talpini, J., Sartori, F., & Savi, M. (2023). A Clustering Strategy for Enhanced FL-Based Intrusion Detection in IoT Networks: Proceedings of the 15th International Conference on Agents and Artificial Intelligence, 152–160. https://doi.org/10.5220/0011627500003393

Tavana, M., & Sorooshian, S. (2024). A systematic review of the soft computing methods shaping the future of the metaverse. *Applied Soft Computing*, *150*, 111098. https://doi.org/10.1016/j.asoc.2023.111098

Thomas, M., Gupta, M. V., Gokul Rajan, V., Rajalakshmi, R., Dixit, R. S., & Choudhary, S. L. (2023). Soft computing in computer network security protection system with

machine learning based on level protection in the cloud environment. Soft Computing. https://doi.org/10.1007/s00500-023-08395-3

Vishwas, B. V. K., & Macharla, S. R. (2025). Time Series Forecasting Using Generative AI: Leveraging AI for Precision Forecasting. Apress. https://doi.org/10.1007/979-8-8688-1276-7

Voloşencu, C. (2024). Introductory chapter: ANFIS for modeling multivariable nonlinear functions. In C. Voloşencu (Ed.), Adaptive Neuro-Fuzzy Inference System as a Universal Estimator. IntechOpen. https://doi.org/10.5772/intechopen.1004337

Wadsworth, A., Thanoon, M. I., McCurry, C., & Sabatto, S. Z. (2019). Development of IIoT Monitoring and Control Security Scheme for Cyber Physical Systems. 2019 SoutheastCon, 1–5. https://doi.org/10.1109/SoutheastCon42311.2019.9020516

Wai, E., & Lee, C. K. M. (2024). Depth in Defense: A Multi-layered Approach to Cybersecurity for SCADA Systems in Industry 4.0. In Dr. L. W. Santoso (Ed.), Science and Technology: Recent Updates and Future Prospects Vol. 2 (pp. 124–144). B P International. https://doi.org/10.9734/bpi/strufp/v2/12542F

Wirsansky, E. (2024). Hands-on genetic algorithms with Python: Applying genetic algorithms to solve real-world AI and machine learning problems. Packt Publishing.

Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77, 103201. https://doi.org/10.1016/j.micpro.2020.103201

Zadeh, L. A. (1994). Soft computing and fuzzy logic. IEEE Software, 11(6), 48–56. https://doi.org/10.1109/52.329401

Zhao, S. (2025). Mathematical Foundations of Reinforcement Learning. Springer Nature Singapore. https://doi.org/10.1007/978-981-97-3944-8

Zolghadr-Asli, B. (2023). Computational Intelligence-based Optimization Algorithms: From Theory to Practice (1st ed.). CRC Press. https://doi.org/10.1201/9781003424765

TEZ ÖĞRENCİSİNE AİT BİLİMSEL ÇIKTILAR

Makaleler

1. Atıcı, S., & Tuna, G. (2025). A deterministic approach to modelling the dynamics of vulnerabilities, cyberattacks, and security hardening using Lotka–Volterra equations. *The Journal of Supercomputing*, *81*(8), 1000. https://doi.org/10.1007/s11227-025-07393-6

Kitaplar / Kitap Bölümleri

1. Atıcı, S., & Tuna, G. (2025). Impact of cybersecurity attacks on electrical system operation. In *Cyber Security Solutions for Protecting and Building the Future Smart Grid* (pp. 117–160). Elsevier. https://doi.org/10.1016/B978-0-443-14066-2.00008-6

ÖZGEÇMİŞ

Sinan Atıcı, lisans eğitimini Kocaeli Üniversitesi Mühendislik Fakültesi Mekatronik Mühendisliği bölümünde tamamlamıştır. 2023 yılından itibaren SecHard Bilgi Teknolojileri şirketinde yazılım geliştirici olarak görev almaktadır. Şu anda Trakya Üniversitesi Mekatronik Mühendisliği programında yüksek lisans öğrenimine devam etmektedir.