



**T.C.  
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**



**YÜKSEK LİSANS TEZİ**

**TÜRKİYE’NİN SİBER GÜVENLİK POLİTİKALARININ YAZILIM  
MÜHENDİSLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ ve KRİTİK  
ALTYAPILARIN SİBER SALDIRILARDAN KORUNMASINA YÖNELİK OLAY  
YÖNETİM SİSTEMİ TASARIMI**

**Uğur GÜRTÜRK**

**DANIŞMAN**

**Dr. Öğr. Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN**

**Bilgisayar Mühendisliği Anabilim Dalı**

**Bilgisayar Mühendisliği Programı**

**Haziran, 2022**

## TEZ KABUL VE ONAYI

Uğur GÜRTÜRK tarafından, Dr. Öğr. Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN danışmanlığında hazırlanan "TÜRKİYE’NİN SİBER GÜVENLİK POLİTİKALARININ YAZILIM MÜHENDİSLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ ve KRİTİK ALTYAPILARIN SİBER SALDIRILARDAN KORUNMASINA YÖNELİK OLAY YÖNETİM SİSTEMİ TASARIMI" başlıklı bu çalışma, jürimiz tarafından 20/06/2022 tarihinde yapılan sınav sonucunda **oy birliği** ile başarılı bulunarak **Yüksek Lisans Tezi** olarak kabul edilmiştir.

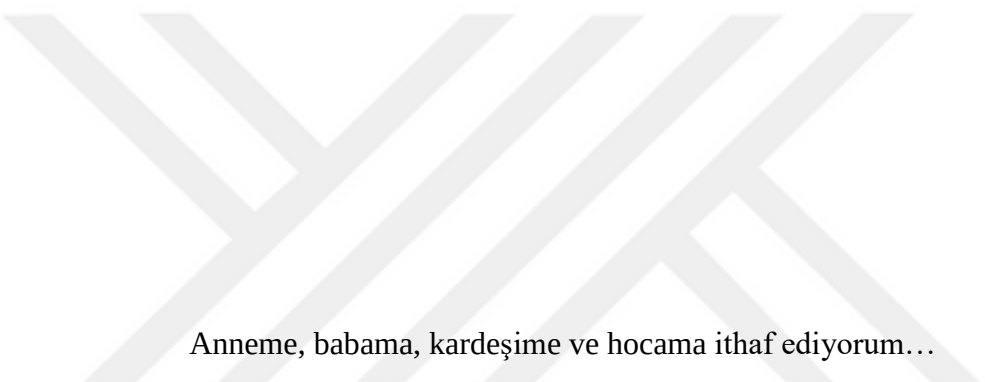
### Tez Jürisi

|          | İmza                                      | Sonuç                               |
|----------|-------------------------------------------|-------------------------------------|
| DANIŞMAN | Dr. Öğr. Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN | <input checked="" type="checkbox"/> |
|          | İstanbul Üniversitesi-Cerrahpaşa          | Kabul                               |
|          | Bilgisayar Mühendisliği Anabilim Dalı     | <input type="checkbox"/><br>Ret     |
| ÜYE      | Dr. Öğr. Üyesi Şafak DURUKAN ODABAŞI      | <input checked="" type="checkbox"/> |
|          | İstanbul Üniversitesi-Cerrahpaşa          | Kabul                               |
|          | Bilgisayar Mühendisliği Anabilim Dalı     | <input type="checkbox"/><br>Ret     |
| ÜYE      | Doç. Dr. Can EYÜPOĞLU                     | <input checked="" type="checkbox"/> |
|          | Millî Savunma Üniversitesi                | Kabul                               |
|          | Bilgisayar Mühendisliği Anabilim Dalı     | <input type="checkbox"/><br>Ret     |

## BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve bilimsel etik kuralları içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını ve her türlü hukuki sorumluluğu aldığımı kabul ederim.

Uğur GÜRTÜRK



Anneme, babama, kardeşime ve hocama ithaf ediyorum...

## **BÜTÇE DESTEKLERİ**

### **TÜRKİYE’NİN SİBER GÜVENLİK POLİTİKALARININ YAZILIM MÜHENDİSLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ ve KRİTİK ALTYAPILARIN SİBER SALDIRILARDAN KORUNMASINA YÖNELİK OLAY YÖNETİM SİSTEMİ TASARIMI**

Bu tez çalışması için herhangi bir kurumdan bütçe desteği alınmamıştır.



## TEŞEKKÜR

Çalışmalarım boyunca beni yönlendiren, bana araştırma olanağı sunan, bilgi ve geniş hoşgörüsü ile benden hiçbir desteğini esirgemeyen değerli danışman hocam Dr.Öğr.Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN'a ve benden maddi, manevi hiçbir desteğini esirgemeyen aileme teşekkürü bir borç bilirim.

Haziran 2022

Uğur GÜRTÜRK



# İÇİNDEKİLER

Sayfa No

|                                                                                                 |      |
|-------------------------------------------------------------------------------------------------|------|
| TEZ KABUL VE ONAYI.....                                                                         | ii   |
| BEYAN .....                                                                                     | iii  |
| BÜTÇE DESTEKLERİ .....                                                                          | v    |
| TEŞEKKÜR.....                                                                                   | vi   |
| İÇİNDEKİLER.....                                                                                | vii  |
| ŞEKİL LİSTESİ .....                                                                             | ix   |
| TABLO LİSTESİ.....                                                                              | xi   |
| SİMGE VE KISALTMA LİSTESİ .....                                                                 | xii  |
| ÖZET .....                                                                                      | xv   |
| ABSTRACT .....                                                                                  | xvii |
| 1. GİRİŞ.....                                                                                   | 1    |
| 2. KAVRAMSAL ÇERÇEVE .....                                                                      | 6    |
| 2.1. ÜLKELERİN SİBER GÜVENLİK POLİTİKALARININ DEĞERLENDİRİLMESİ<br>VE İLGİLİ ÇALIŞMALAR .....   | 6    |
| 2.1.1. Yazılım Mühendisliği ve Türkiye'nin Siber Güvenlik Politikaları.....                     | 20   |
| 2.1.2. İlgili Çalışmalar.....                                                                   | 36   |
| 2.2. KRİTİK YAPILARDA GÜVENLİK BİLGİLERİ VE OLAY YÖNETİMİ .....                                 | 45   |
| 2.3. VERİ SETİ İLE İLGİLİ ÇALIŞMALAR.....                                                       | 50   |
| 3. YÖNTEM.....                                                                                  | 62   |
| 3.1. KULLANILAN YÖNTEMLER.....                                                                  | 64   |
| 3.1.1. Destek Vektör Makinesi Sınıflandırıcısı (Support Vector Machine Classifier-SVM)<br>..... | 64   |
| 3.1.2. Lojistik Regresyon Sınıflandırıcısı (Logistic Regression Classifier-LR) .....            | 65   |
| 3.1.3. Rastgele Orman Sınıflandırıcısı (Random Forest Classifier-RF) .....                      | 66   |
| 3.1.4. Extra Ağaçlar Sınıflandırıcısı (Extra Trees Classifier-XT).....                          | 67   |
| 3.1.5. K- En Yakın Komşu Sınıflandırıcısı (K- Nearest Neighbour Classifier-KNN).....            | 67   |
| 3.1.6. Karar Ağaçları Sınıflandırıcısı (Decision Tree Classifier-DT) .....                      | 68   |
| 3.1.7. Bayes Ağları Sınıflandırıcısı (Bayesian Network Classifier-BayesNet).....                | 69   |

|                                                                                 |            |
|---------------------------------------------------------------------------------|------------|
| 3.1.8. Naive Bayes Sınıflandırıcısı (Naive Bayes Classifier-NB).....            | 70         |
| 3.1.9. J48 Karar Ağacı Sınıflandırıcısı (J48 Decision Tree Classifier-J48)..... | 71         |
| 3.2. KULLANILAN VERİ SETİ.....                                                  | 72         |
| 3.3. VERİ SETİNDE YER ALAN SALDIRI TÜRLERİ.....                                 | 74         |
| 3.3.1. Fuzzer Saldırıları .....                                                 | 74         |
| 3.3.2. Analysis (Analiz) Saldırıları.....                                       | 74         |
| 3.3.3. Backdoor (Arka Kapı) Saldırıları .....                                   | 75         |
| 3.3.4. Hizmet Reddi (Denial of Service-DoS) Saldırıları .....                   | 75         |
| 3.3.5. Exploit (İstismar) Saldırıları.....                                      | 75         |
| 3.3.6. Generic (Genel) Saldırıları .....                                        | 76         |
| 3.3.7. Reconnaissance (Keşif) Saldırıları .....                                 | 76         |
| 3.3.8. Shellcode (Kabuk Kodu) Saldırıları .....                                 | 76         |
| 3.3.9. Worm (Solucan) Saldırıları .....                                         | 76         |
| 3.4. KULLANILAN ARAÇLAR VE GELİŞTİRME ORTAMI .....                              | 76         |
| 3.5. GERÇEKLENEN SİSTEM .....                                                   | 79         |
| 3.5.1. Veri Seti Değerlendirmesi .....                                          | 80         |
| 3.5.2. Kullanılan Kütüphaneler .....                                            | 81         |
| 3.5.3. Uygulanan Yöntem ve Ön İşleme .....                                      | 82         |
| 3.5.4. Sınıflandırma.....                                                       | 85         |
| <b>4. BULGULAR .....</b>                                                        | <b>93</b>  |
| <b>5. TARTIŞMA.....</b>                                                         | <b>98</b>  |
| <b>6. SONUÇ VE ÖNERİLER .....</b>                                               | <b>102</b> |
| <b>KAYNAKLAR.....</b>                                                           | <b>106</b> |
| <b>ETİK KURUL İZİN YAZISI .....</b>                                             | <b>114</b> |
| <b>KURUM İZNİ YAZILARI.....</b>                                                 | <b>115</b> |
| <b>ÖZGEÇMİŞ .....</b>                                                           | <b>116</b> |

## ŞEKİL LİSTESİ

### Sayfa No

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Şekil 1.1: Kritik altyapı sistemleri .....                                       | 1  |
| Şekil 1.2: Türkiye’de bilişim alanında kritik altyapılara örnekler.....          | 4  |
| Şekil 1.3: Güvenlik değerlendirmesi .....                                        | 5  |
| Şekil 2.1: Ülkelerin siber güvenlik politika yayımlama zaman çizelgesi [28]..... | 9  |
| Şekil 2.2: Güvenlik yöntem değerlendirmesi .....                                 | 46 |
| Şekil 2.3: Güvenlik zafiyet türleri .....                                        | 47 |
| Şekil 2.4: Güvenlik zafiyet türleri .....                                        | 48 |
| Şekil 3.1: Veri analizi işlem adımları [105] .....                               | 63 |
| Şekil 3.2: SVM'nin genel mimarisi [111].....                                     | 65 |
| Şekil 3.3: LR'nin genel mimarisi [115] .....                                     | 66 |
| Şekil 3.4: XT işleyiş mimarisi [112] .....                                       | 67 |
| Şekil 3.5: KNN temel mantıksal yapısı [73].....                                  | 68 |
| Şekil 3.6: Sınıflandırma yöntemleri geliştirme zaman çizelgesi .....             | 71 |
| Şekil 3.7: Google Colabratory arayüzü [107].....                                 | 78 |
| Şekil 3.8: Tez çalışmasının genel içerik diyagramı .....                         | 79 |
| Şekil 3.9: Veri setinin saldırılara göre dağılımı.....                           | 80 |
| Şekil 3.10: Eğitim ve test veri setlerindeki protokol dağılımı .....             | 80 |
| Şekil 3.11: Eğitim veri setindeki normal ve saldırı verilerinin oranları .....   | 81 |
| Şekil 3.12: Veri seti korelasyon matrisi .....                                   | 89 |
| Şekil 3.13: Uygulama genel diyagramı .....                                       | 90 |
| Şekil 4.1: Colab uygulaması sınıflandırma başarımlar oranları .....              | 93 |
| Şekil 4.2: Weka analizi sınıflandırma başarımlar oranları .....                  | 93 |

|                                                        |     |
|--------------------------------------------------------|-----|
| Şekil 4.3: Uygulanan akış şeması.....                  | 95  |
| Şekil 4.4: Ön işlemeziz sınıflandırma sonucu (LR)..... | 97  |
| Şekil 5.1: İncelenen sistemin kavramsal çerçevesi..... | 100 |



## TABLO LİSTESİ

### Sayfa No

|                                                                                                |    |
|------------------------------------------------------------------------------------------------|----|
| Tablo 2.1: Yüksek siber güvenlik seviyelerine sahip gelişmiş ülkeler sıralaması .....          | 7  |
| Tablo 2.2: Yüksek siber güvenlik seviyelerine sahip gelişmekte olan ülkeler sıralaması .....   | 8  |
| Tablo 2.3: Gerçekleşen büyük siber olaylara örnekler [23] .....                                | 20 |
| Tablo 2.4: Türkiye’de dijitalleşme ve siber güvenlik faaliyetleri alanında önemli adımlar..... | 21 |
| Tablo 2.5: Türkiye’nin dijitalleşme ve siber güvenlik faaliyetleri alanında önemli adımları .. | 24 |
| Tablo 2.6: E-Türkiye Girişimi neticesinde çalışmalar ve sorumlu kurumlar .....                 | 25 |
| Tablo 2.7: Siber Güvenlik Kurulu’nun teşkilatı ve görevleri .....                              | 26 |
| Tablo 2.8: 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 1 .....                   | 27 |
| Tablo 2.9: 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 2 .....                   | 27 |
| Tablo 2.10: 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 3 .....                  | 28 |
| Tablo 2.11: 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 4 .....                  | 28 |
| Tablo 2.12: Dünyada yazılım mühendisliği eğitiminde en iyi üniversiteler .....                 | 30 |
| Tablo 2.13: Türkiye’de yazılım mühendisliği eğitimi veren üniversiteler .....                  | 30 |
| Tablo 2.14: Veri seti ile ilgili yapılan çalışmaların karşılaştırılması.....                   | 60 |
| Tablo 3.1: UNSW-NB15 veri seti alanları .....                                                  | 73 |
| Tablo 3.2: UNSW-NB15 veri seti alanları (devam) .....                                          | 74 |
| Tablo 3.3: Kullanılan başlıca kütüphaneler .....                                               | 81 |
| Tablo 3.4: Veri setinde en yüksek korelasyona sahip sütunlar.....                              | 89 |
| Tablo 4.1: Uygulamaların genel sonuçları .....                                                 | 94 |
| Tablo 5.1: Çalışmaya benzer en güncel kaynaklar .....                                          | 98 |
| Tablo 5.2: Benzer çalışmalarla başarımların karşılaştırması .....                              | 99 |

## SİMGE VE KISALTMA LİSTESİ

### Simgeler

### Açıklama

|          |                            |
|----------|----------------------------|
| $\Sigma$ | : Sigma (Toplam Dizisi)    |
| $\Pi$    | : Kartezyen Çarpım Sembolü |
| $\pi$    | : Pi Sayısı                |
| $\wedge$ | : Ve Simgesi               |
| $\vee$   | : Ya Da Simgesi            |
| $\Gamma$ | : Gamma Fonksiyonu         |

### Kısaltmalar

### Açıklama

|                |                                                                                                |
|----------------|------------------------------------------------------------------------------------------------|
| <b>DDoS</b>    | : Distributed Denial of Service-Dağıtılmış Hizmet Reddi                                        |
| <b>ITU</b>     | : International Telecommunication Union-Uluslararası Telekomünikasyon Birliği                  |
| <b>ENISA</b>   | : European Network and Information Security Agency-Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı |
| <b>NCSS</b>    | : National Cyber Security Strategy-Ulusal Siber Güvenlik Stratejisi                            |
| <b>CERTS</b>   | : Computer Emergency Response Team-Bilgisayar Acil Müdahale Ekibi                              |
| <b>AR-GE</b>   | : Araştırma ve Geliştirme                                                                      |
| <b>BT</b>      | : Bilişim Teknolojileri                                                                        |
| <b>KVK</b>     | : Kişisel Verilerin Korunması                                                                  |
| <b>CMCA</b>    | : Computer Misuse and Cybersecurity Act-Bilgisayarın Kötüye Kullanımı ve Siber Güvenlik Yasası |
| <b>TÜBİTAK</b> | : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu                                              |
| <b>OKTEM</b>   | : Ortak Kriter Test Merkezi                                                                    |
| <b>TSK</b>     | : Türk Silahlı Kuvvetleri                                                                      |
| <b>DPT</b>     | : Devlet Planlama Teşkilatı                                                                    |
| <b>BTD</b>     | : Bilgi Toplumu Dairesi                                                                        |
| <b>TSE</b>     | : Türk Standartlar Enstitüsü                                                                   |
| <b>SCADA</b>   | : Supervisory Control and Data Acquisition-Denetim Kontrolü ve Veri Toplama                    |
| <b>NATO</b>    | : North Atlantic Treaty Organization-Kuzey Atlantik Antlaşması Örgütü                          |

|              |                                                                                 |
|--------------|---------------------------------------------------------------------------------|
| <b>AFAD</b>  | : Afet ve Acil Durum Yönetimi                                                   |
| <b>CBDDO</b> | : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi                                        |
| <b>CNII</b>  | : Critical National Information Infrastructure-Kritik Ulusal Bilgi Altyapısı    |
| <b>BM</b>    | : Birleşmiş Milletler                                                           |
| <b>MAF</b>   | : Malaysian Armed Forces-Malezya Silahlı Kuvvetleri                             |
| <b>GCC</b>   | : Gulf Cooperation Council-Körfez İşbirliği Konferansı                          |
| <b>ABD</b>   | : Amerika Birleşik Devletleri                                                   |
| <b>SIEM</b>  | : Security Information and Event Management-Güvenlik Bilgileri ve Olay Yönetimi |
| <b>SSL</b>   | : Secure Sockets Layer-Güvenli Soket Katmanı                                    |
| <b>TLS</b>   | : Transport Layer Security-Taşıma Katmanı Güvenliği                             |
| <b>TTP</b>   | : Tetkit, Teknik ve Değerlendirme                                               |
| <b>UEBA</b>  | : User And Entity Behavior Analytics-Kullanıcı ve Varlık Davranışı Analitiği    |
| <b>MTTD</b>  | : Mean Time to Detect-Ortalama Algılama Süresi                                  |
| <b>MTTR</b>  | : Mean Time to Response-Ortalama Yanıtlama Süresi                               |
| <b>STS</b>   | : Saldırı Tespit Sistemi                                                        |
| <b>SMOTE</b> | : Synthetic Minority Oversampling Technique-Azınlık Aşırı Örnekleme Tekniği     |
| <b>ROC</b>   | : Receiver Operating Characteristic-Alıcı Çalışma Karakteristiği                |
| <b>PRC</b>   | : Precision-Recall Curves-Hassas-Geri Çağırma Eğrileri                          |
| <b>PCA</b>   | : Principal Component Analysis-Temel Bileşenler Analizi                         |
| <b>KNN</b>   | : K-Nearest Neighbors Algorithm-En Yakın Komşular Algoritması                   |
| <b>SGD</b>   | : Stochastic Gradient Descent-Stokastik Gradyan Azalma                          |
| <b>RF</b>    | : Random Forest Algorithm-Rastgele Orman Algoritması                            |
| <b>LR</b>    | : Logistic Regression Algorithm-Lojistik Regresyon Algoritması                  |
| <b>NB</b>    | : Naive Bayes Algorithm-Naive Bayes Algoritması                                 |
| <b>BN</b>    | : Bayesian Network Algorithm-BayesNet Algoritması                               |
| <b>IoT</b>   | : Internet of Things-Nesnelerin İnterneti                                       |
| <b>MLP</b>   | : Multi-layer Perceptron-Çok Katmanlı Algılayıcı                                |
| <b>SVM</b>   | : Support Vector Machines-Destek Vektör Makineleri                              |
| <b>DT</b>    | : Decision Tree-Karar Ağaçları                                                  |
| <b>XT</b>    | : Extra Trees-Ekstra Ağaçlar                                                    |
| <b>ELM</b>   | : Extreme Learning Machines-Aşırı Öğrenme Makinesi                              |
| <b>MSE</b>   | : Mean Squared Error-Ortalama Kare Hata                                         |

|                |                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------|
| <b>FPR</b>     | : False Positive Rate-Yanlış Pozitif Oranı                                                                 |
| <b>TPR</b>     | : True Positive Rate-Gerçek Pozitif Oranı                                                                  |
| <b>LSTM</b>    | : Long Short Term Memory-Uzun Kısa Süreli Bellek                                                           |
| <b>GRU</b>     | : Gated Recurrent Unit-Geçitli Tekrarlayan Birimler                                                        |
| <b>DNN</b>     | : Deep Neural Networks-Derin Sinir Ağları                                                                  |
| <b>FSAP</b>    | : Feature Selection Approach-Özellik Seçimi Yaklaşımı                                                      |
| <b>SABADT</b>  | : Signature and Anomaly Based Attack Detection Technique-İmza ve Anomali Tabanlı Saldırı Tespit Tekniği    |
| <b>RBFN</b>    | : Radial Basis Function Networks-Radyal Temel İşlev Ağı                                                    |
| <b>BPN</b>     | : Backpropagation Neural Network-Geri Yayımlı Sinir Ağı                                                    |
| <b>TCP</b>     | : Transmission Control Protocol-İletim Kontrol Protokolü                                                   |
| <b>UDP</b>     | : User Datagram Protocol-Kullanıcı Datagram Protokolü                                                      |
| <b>DoS</b>     | : Denial-of-Service-Hizmet Reddi                                                                           |
| <b>ML</b>      | : Machine Learning-Makine Öğrenimi                                                                         |
| <b>NIDS</b>    | : Network Intrusion Detection System-Ağ Saldırı Tespit Sistemi                                             |
| <b>GUI</b>     | : Graphical User Interface-Grafiksel Kullanıcı Arayüzü                                                     |
| <b>DL</b>      | : Deep Learning-Derin Öğrenme                                                                              |
| <b>CM</b>      | : Confusion Matrix-Karışıklık Matrisi                                                                      |
| <b>NSA</b>     | : National Security Agency-Ulusal Güvenlik Ajansı                                                          |
| <b>UK</b>      | : United Kingdom-Birleşik Krallık                                                                          |
| <b>BSSN</b>    | : National Cyber and Crypto Agency-Ulusal Siber ve Şifreleme Ajansı                                        |
| <b>NCSP</b>    | : Malaysia's National Cyber Security Policy-Malezya'nın Ulusal Siber Güvenlik Politikası                   |
| <b>SaE-ELM</b> | : Self-Adaptive Evolutionary Extreme Learning Machine-Kendinden Uyarlamalı Evrimsel Aşırı Öğrenme Makinesi |
| <b>NN</b>      | : Neural Networks-Yapay Sinir Ağları                                                                       |
| <b>PPO</b>     | : Proximal Policy Optimization-Yakınsal Politika Optimizasyonu                                             |
| <b>IDHCS</b>   | : Intrusion Detection Hyperparameter Control System-Saldırı Tespit Hiperparametre Kontrol Sistemi          |
| <b>RNN</b>     | : Recurrent Neural Network-Yinelemeli Sinir Ağı                                                            |
| <b>TBMM</b>    | : Türkiye Büyük Millet Meclisi                                                                             |
| <b>AUC</b>     | : Area Under Curve-ROC Eğrisi Altındaki Alan                                                               |
| <b>CPU</b>     | : Central Process Unit-Merkezi İşlem Birimi                                                                |
| <b>HTML</b>    | : HyperText Markup Language-Hiper Metin İşaretleme Dili                                                    |
| <b>URL</b>     | : Uniform Resource Locator-Tekdüzen Kaynak Bulucu                                                          |

## ÖZET

### YÜKSEK LİSANS TEZİ

TÜRKİYE’NİN SİBER GÜVENLİK POLİTİKALARININ YAZILIM MÜHENDİSLİĞİ  
AÇISINDAN DEĞERLENDİRİLMESİ ve KRİTİK ALTYAPILARIN SİBER  
SALDIRILARDAN KORUNMASINA YÖNELİK OLAY YÖNETİM SİSTEMİ TASARIMI

Uğur GÜRTÜRK

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Danışman : Dr. Öğr. Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN

Bilgi ve bilgi sistemleri güvenliğinin öneminin hızla gelişen teknoloji ile birlikte artması, alınması gereken tedbirlerin gerekliliğini de en üst düzeye çıkartmıştır. Bilgi güvenliği sistemlerinde kullanılan araçlar çok çeşitli ve güçlü olsa da, gelişen yeni teknolojilerden kaynaklanan yeni güvenlik açıklıklarını bulma noktasında başarılı olamayabilmektedir. Kötücül girişimlerden önce saldırganların nasıl saldırabileceğini tespit etmek ve buna göre güvenliği sağlamak, alınan tedbirlerin etkisini en yüksek seviyeye çıkaracaktır.

Kritik altyapı sistemleri, gelişen teknoloji ile birlikte modern toplumların temelini oluşturmaktadır ve ulusal refahın korunması için önem arz eden yapılardır. Genellikle tarım, su, elektrik şebekesi, ulaşım, iletişim ve teknoloji sistemleri ile çeşitli kamu ve özel sektör yapılarını içeren bu sektörler günlük hayatın devamını sağlamak için son derecede elzemdir. Birbirine bağlı ve bağımlı hale gelen karmaşık sistemler olan bu yapıların sadece bir parçasının arızalanması bile diğer bağımlı sistemlerin arızalanmasına neden olmakta ve arızanın meydana geldiği altyapıyı tümüyle etkileyebilmektedir. Ayrıca, devletlerin güvenliği, ekonomisi ve vatandaşların refahı için tehlikeli sonuçlar meydana gelebilmektedir. Bu nedenler göz önüne alındığında kritik altyapıların güvenliğinin sağlanması siber güvenlik çatısı altında hayati bir rol taşımaktadır ve bu tür altyapıların güvenliği Türkiye’de tam olarak önemli bir siber güvenlik sorunu olarak görülmemektedir. Kritik altyapının korunmasına ilişkin sorunlar, siber güvenlik konusundaki çalışmaların gölgesinde kalmaya devam etmektedir.

Son yıllarda bilgi güvenliğine yönelik tehditler, dünyada aktif olarak kullanılan hizmetlere yönelik istismlarların ve tehditlerin şirketler için bir kâr modeli haline gelmesi nedeniyle daha hedef odaklı bir hale gelmiştir. Güvenlik Bilgileri ve Olay Yönetimi (SIEM), Güvenlik bilgileri ve olay yönetimi anlamına gelmekte olup ağ ve güvenlik cihazlarından veri toplama ve analiz etme yeteneklerine sahiptir. SIEM, günümüzde birçok siber güvenlik operasyon merkezinin kullandığı izleme yeteneklerini geliştirmek için çeşitli güvenlik cihazlarından gelen olayları ilişkilendirmek için tüm önemli bilgileri birleştirilmiş bir çerçevede toplamak için kullanılan bir yöntemdir.

Bu tez çalışmasında, öncelikle kritik altyapı tanımına ve detaylarına yer verilmiş; bu yapıların korunmasına yönelik öncelikle Türkiye’de önlem alınması aşamasında bir farkındalık oluşturmak amaçlanmıştır. Daha sonra ülkelerin siber güvenlik politikaları ilişkisel bir yapıda verilmiş; gerçekleştirilen çalışmalar ve politikalar birçok kapsamda değerlendirilmiştir. Türkiye’nin siber güvenlik alanındaki politikaları incelenerek, bu anlamda geliştirilen çalışmalara ve hukuksal çalışmalarına yer verilmiştir. Ayrıca bir bütün olarak da değerlendirilebilen kritik altyapı-SIEM ilişkisi ve teknolojik gelişmelerin bir zorunluluğu sonucu olarak yazılım mühendisliği kavramı ele alınmış; ulusal ve uluslararası anlamda yazılım mühendisliği hakkında bilgiler verilmiştir. Kritik altyapı, siber güvenlik politikaları ve SIEM’i içeren güncel çalışmalara da kapsamlı bir şekilde yer verilmiştir. Tez çalışmasının uygulama bölümünde ise gerçek hayattaki modern normal senaryoların yanı sıra ağ trafiğinden elde edilen verilerden ve çeşitli saldırı aktivitelerinden oluşan “UNSW\_NB15” veri seti kullanılarak uygulama geliştirilmiştir.

Çalışmalar ile “Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode ve Worms” olmak üzere dokuz tür saldırı türü ve “Normal” aktivitelerden oluşan kategori ile toplamda 10 farklı kategoriye ait analiz gerçekleştirilmiştir. Çalışma temel yapı olarak ikiye ayrılmaktadır. İlk adım Google Colabratory üzerinde gerçekleştirilmiş olup daha sonra ise Weka’da bir takım deneysel çalışmalar gerçekleştirilmiştir. Google Colabratory uygulamasında LR, XT, SVM, RF ve DT yöntemleri ile sınıflandırmalar gerçekleştirilmiştir. Google Colabratory ile geliştirilen uygulamada Rastgele Orman Sınıflandırıcısı (Random Forest-RF)’nda %98,62, Karar Ağaçları (Decision Tree-DT)’nda %99,10, Lojistik Regresyon (Logistic Regression-LR)’da 98,87, Ekstra Ağaçlar (Extra Trees-XT)’da %95,13 ve Destek Vektör Makineleri (Support Vector Machines-SVM)’nde %99,12 başarı elde edilmiştir. Daha sonra Weka’da yapılan çalışmalar ve deneyler sonucunda RF’de %92,05, DT’de %100, KNN’de %100, J48’de %100, NB’de %99,19 ve BayesNet’de %99,35 başarı elde edilmiştir. |

Haziran 2022 , |134| sayfa.

**Anahtar kelimeler:** Kritik Altyapıların Korunması, Siber Güvenlik, Log Analizi, Yazılım Mühendisliği, Makine Öğrenmesi, SIEM, Siber Güvenlik Politikaları|

## **ABSTRACT**

**M.Sc. THESIS**

**EVALUATION OF TÜRKİYE'S CYBER SECURITY POLICIES IN TERMS OF  
SOFTWARE ENGINEERING AND INCIDENT MANAGEMENT SYSTEM DESIGN FOR  
THE PROTECTION OF CRITICAL INFRASTRUCTURES FROM CYBER ATTACKS**

**Uğur GÜRTÜRK**

**İstanbul University-Cerrahpaşa**

**Institute of Graduate Studies**

**Department of Computer Engineering**

**Computer Engineering**

**Supervisor : Assist. Prof. Dr. Gülsüm Zeynep GÜRKAŞ AYDIN**

The increase in the importance of information and information systems security with the rapidly developing technology has also brought the necessity of the measures to be taken to the highest level. Although the tools used in information security systems are very diverse and powerful, they may not be successful in finding new security vulnerabilities arising from developing new technologies. Identifying how attackers can attack before malicious attempts and providing security accordingly will maximize the effectiveness of the measures taken.

Critical infrastructure systems, together with developing technology, form the basis of modern societies and are important structures for the protection of national welfare. These sectors, which generally include agriculture, water, electricity grid, transportation, communication and technology systems and various public and private sector structures, are extremely essential to ensure the continuation of daily life. Even the failure of only a part of these structures, which are complex systems that are interconnected and dependent, causes the failure of other dependent systems and can affect the entire infrastructure where the failure occurred. In addition, dangerous consequences may occur for the security of states, the economy and the welfare of citizens. Considering these reasons, ensuring the security of critical infrastructures plays a vital role under the roof of cyber security and the security of such infrastructures is not exactly seen as an important cyber security problem in Türkiye. Problems related to the protection of critical infrastructure continue to be overshadowed by studies on cybersecurity.

In recent years, threats to information security have become more target-oriented, as exploits and threats to services actively used in the world have become a profit model for companies. Security Information and Event Management (SIEM) stands for Security information and event management and has the capabilities to collect and analyze data from network and security devices. SIEM is a method used to gather all important information in a unified framework to correlate events from various security devices to enhance the monitoring capabilities used by many cybersecurity operations centers today.

In this thesis, first of all, the definition and details of critical infrastructure are given; It is aimed to raise awareness in the process of taking precautions in Türkiye for the protection of these structures. Then, the cyber security policies of the countries are given in a relational structure; The studies and policies carried out have been evaluated in many contexts. By examining Türkiye's policies in the field of cyber security, studies and legal studies developed in this sense are included. In addition, the critical infrastructure-SIEM relationship, which can also be evaluated as a whole, and the concept of software engineering as a result of technological developments are discussed; National and international information about software engineering is given. Current studies including critical infrastructure, cyber security policies and SIEM are also covered extensively. In the application part of the thesis, the application was developed using the “UNSW\_NB15” dataset, which consists of data obtained from network traffic and various attack activities, as well as real-life modern normal scenarios.

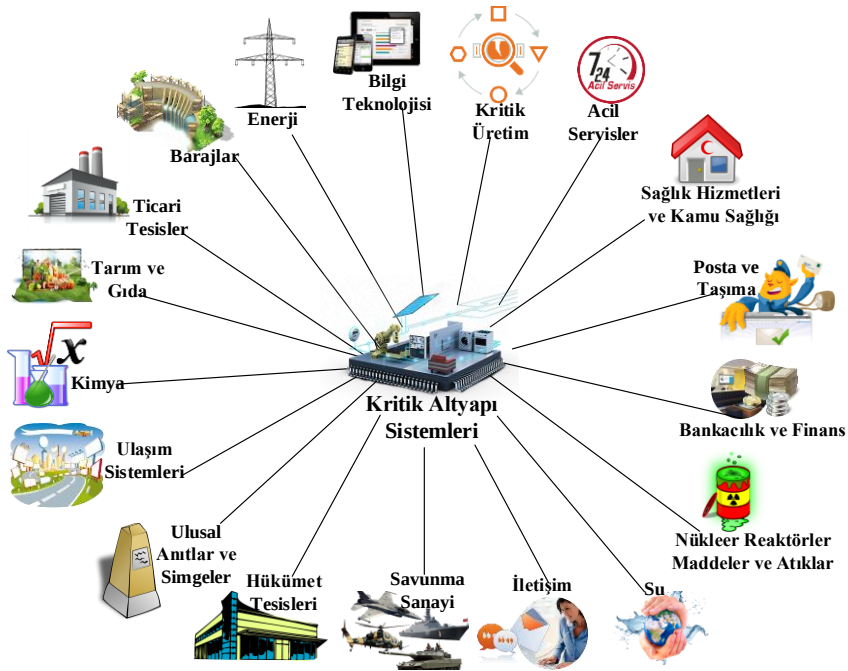
With the studies, a total of 10 different categories were analyzed with the category consisting of nine types of attacks, namely "Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode and Worms", and "Normal" activities. The study is divided into two as the basic structure. The first step was carried out on Google Colab, and then some experimental studies were carried out in Weka. Classifications were made using LR, XT, SVM, RF and DT methods in the Google Colab application. In the application developed with Google Colab, 98.62% in Random Forest Classifier (Random Forest-RF), 99.10% in Decision Tree-DT, 98.87% in Logistic Regression-LR, 95.13% success was achieved in Extra Trees (XT) and 99.12% success in Support Vector Machines (SVM). As a result of the studies and experiments carried out in Weka, 92.05% in RF, 100% in DT, 100% in KNN, 100% in J48, 99.19% in NB and 99.35% in BayesNet achievements achieved.

June 2022, 134 pages.

**Keywords:** Protection of Critical Infrastructure, Cyber Security, Log Analysis, Software Engineering, Machine Learning, SIEM, Cyber Security Policies

## 1. GİRİŞ

Kritik altyapı, bir ulusun güvenliğini, ekonomisini, halkın refahını, güvenliğini sağlamak için sürekli çalışmasının gerekli olduğu önemli yapılar, sistemler, ağlar ve varlıklar bütünü olarak tanımlanmaktadır. Kritik altyapı, birbirine bağlı ve bağımlı hale gelen karmaşık sistemleri temsil etmektedir. “Kritik Altyapı” terimi ilk olarak 1996 yılında Amerika Birleşik Devletleri (ABD) Başkanı tarafından kullanılmıştır. Kritik altyapı sistemleri modern toplumların temelini oluşturmaktadır ve ulusal refahın korunması için son derece önem arz etmektedir. Altyapının sadece bir parçasının arızalanması bile diğer bağımlı sistemlerin arızalanmasına neden olmaktadır ve bu da arızanın meydana geldiği altyapıyı tümüyle etkileyebilmektedir. Böyle bir durumda ve ortamda, altyapının esnekliği ve güvenliği ulusal bir öncelik haline gelmektedir. Kritik altyapının sağladığı hizmetlerde veya operasyonlarda herhangi bir hasar veya kesinti olduğunda, devletlerin güvenliği, ekonomisi ve ayrıca vatandaşların refahı için potansiyel olarak tehlikeli sonuçlar meydana gelebilmektedir. Kritik altyapı sistemlerinin kapsamı geniş olsa da bu sistemler genellikle tarım, su, elektrik şebekesi, ulaşım, iletişim ve teknoloji sistemleri, çeşitli kamu ve özel sektör gibi yapılarını içermektedir. Bu sektörler günlük hayatın devamını sağlamak için son derecede elzemdir. [1, 2].



Şekil 1.1: Kritik altyapı sistemleri

Şekil 1.1, en önemli kritik altyapı sistemi türlerini göstermektedir. Kritik altyapı güvenliği esas olarak siber güvenlik ile birlikte ele alınmaktadır. Kritik altyapı sektörlerine, özellikle de enerji ile ilgili sektörler için siber saldırıların gün geçtikçe arttığı gözlemlenmektedir. Sebepler genellikle sistemlerin kapatılması, hizmetlerin ve operasyonların kesintiye uğraması veya siber saldırganların etkilenen sistemleri uzaktan kontrol etmesine farkında olmadan izin verilmesidir. Örneğin, 2003 yılında ABD, her biri tamamen farklı kritik noktaları hedef alan üç siber saldırı ile karşı karşıya kalmıştır. Ağustos ayında ABD'nin Kuzeydoğu Bölgesi ve Ontario Eyaleti, elektrik şirketlerinin sistemlerindeki bir yazılım hatası sonucu yaygın bir elektrik kesintisi yaşarken, aynı ayda bilgisayar solucanı sisteme bulaşmıştır. Ohio'da işletilen Davis-Besse Nükleer Santrali'nin şebekesi, santralin izleme sistemlerini yaklaşık 5 saat çalışamaz hale getirmiştir. Ekim ayında ise ülkenin en işlek limanlarından biri olan Houston'ın bilgisayar sistemi saldırıya uğramıştır ve bu siber saldırının Birleşik Krallık (United Kingdom-UK) lokasyonlu bir bilgisayar tarafından yapıldığı söylenmiştir.

ABD'nin kritik altyapı sistemlerine yönelik siber saldırılar diğer ülkelerde de olduğu gibi yıllar içerisinde artarak devam etmiştir. 2013 yılında Silikon Vadisi'nin elektrik trafo merkezine yapılan bir siber saldırı, bu tür sistemlere verilen zararlara yönelik en büyük örneklerden biri olarak verilebilir [2-4]. ABD İstihbaratı, bu saldırı örnekleriyle altyapıdaki fiziksel hasara dikkat çekerken, ilerleyen yıllarda da ABD'nin başkanlık seçimlerinin sonucunu etkilemek için Rusya'nın 2016 yılında siber yollar kullanmış olabileceğini gündeme getirmiştir.

Kritik altyapıya yönelik siber saldırılar sadece ABD'ye yönelik gerçekleşmemekte, dünyadaki hemen hemen her ülke böyle bir tehdide maruz kalmaktadır. 2007'de Estonya, Tallinn'deki (Ottis) Sovyet dönemi heykeli konusunda Rusya ile yaşanan siyasi çekişme sonucunda yirmi iki gün süren ve Estonya parlamentosu, bakanlıklar, bankalar ve medya merkezleri gibi federal kurumları hedef alan siber saldırılara maruz kalmıştır [5, 6].

Ukrayna, 2015 yılında elektrik şebekelerine yönelik geniş kapsamlı siber saldırıyla karşı karşıya kalan bir başka Avrupa ülkesidir. Kötücül niyetli siber saldırganlar, Rusya'nın enerji dağıtım şirketlerinin bilgi sistemlerini hedef almış ve gerçekleştirilen saldırı ile yaklaşık 6 saat boyunca elektrik akışını kesmişlerdir. 2017 yılında Ukrayna'da ağırlıklı olarak devlet kurumlarını, finans ve medya kurumlarını ve özellikle elektrik tedarikçilerini etkileyen 3 siber saldırı devam ederken, aynı yıl Avustralya, Fransa, Almanya, İtalya, Polonya'da da altyapılara yönelik benzer saldırılar rapor edilmiştir [3-7].

Sık rapor edilmese de Türkiye de, kritik altyapıları hedef alan siber saldırılarla da karşı karşıya kalmaktadır. Örneğin 2003 yılında Batman Barajı'nın bilgisayarları bir Alman

fırmasınca kilitlenmiş ve bu saldırı nedeniyle firma ödemesini alamamıştır. Ocak 2009'da birçok ülkenin bilgisayar sistemlerine bulaşan Conficker adlı bilgisayar virüsü, aynı zamanda Atatürk Havalimanı'nın sistemlerini de etkilemiştir [3].

Bunlara ek olarak 2019 yılının sonlarına doğru özellikle “Dağıtılmış Hizmet Reddi” (Distributed Denial of Service - DDoS) saldırısı başta olmak üzere bilinmeyen bir siber saldırı yaşanmıştır. DDoS, internete bağlı bir sistemin hizmetlerini, bir bilgisayar veya ağ kaynaklarına gerçek kullanıcılar tarafından erişilemeyecek şekilde geçici veya süresiz olarak kesintiye uğratmayı amaçlayan bir siber saldırıdır. Bu saldırı Türkiye'deki bankacılık ve telekomünikasyon sektörlerini de bu tanımda belirtilen amaçla hedef almıştır. Kritik altyapı sistemlerine yönelik siber tehditlerin önümüzdeki yıllarda artması beklenmektedir. Özellikle batılı hükümetler, yasal, idari ve kurumsal alanlarda ilerici adımlar atarak kritik altyapı koruma alanına ciddi şekilde odaklanmaya başlamışlardır [1-9].

Kritik altyapı güvenliği gelişmiş ülkelerin en önemli gündem maddelerinden biri olmasına rağmen Türkiye'de bu alanda çalışmalar olması gereken nitelikte ve yeterlilikte değildir. Kritik altyapıların güvenliğinin sağlanması siber güvenlik çatısı altında hayati bir rol taşımaktadır ve bu tür altyapıların güvenliği Türkiye'de önemli bir siber güvenlik sorunu olarak görülmemektedir. Kritik altyapı korumasına ilişkin sorunlar, siber güvenlik konusundaki çalışmaların gölgesinde kalmaya devam etmektedir.

Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU)'ne göre siber güvenlik, siber saldırılara karşı alınması gereken önlemler bütünüdür. Ayrıca kurum, kuruluş ve kullanıcıların varlıklarını korumak için geliştirdikleri politikalar, araçlar, sistemler ve uygulamalar; bilişim alanında kullanılan yazılı belgeler, elektronik medya belgeleri, etkinlikler, eğitimler ve güvenlik teknolojileri siber güvenliğin unsurları arasında yer almaktadır [9-11].



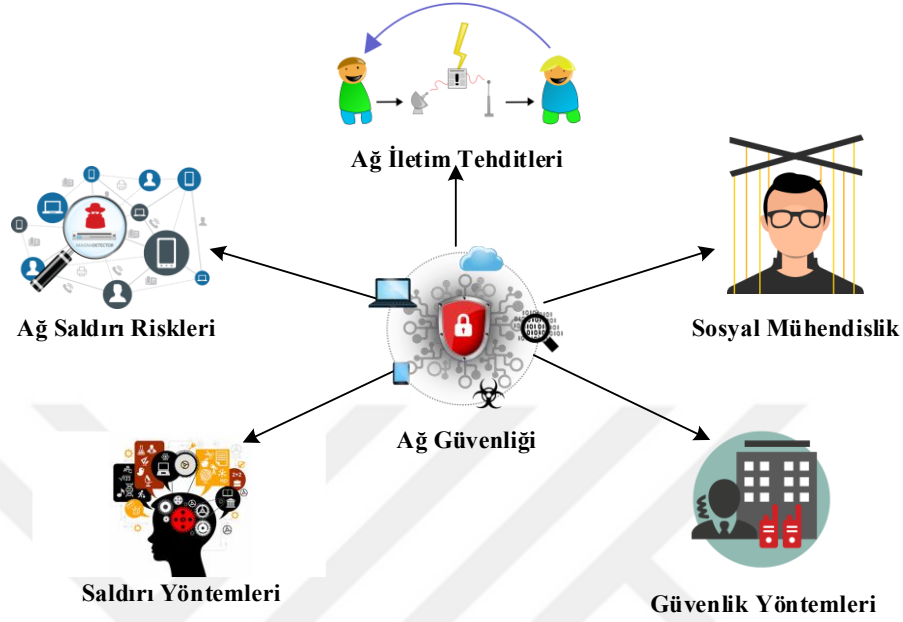
**Şekil 1.2:** Türkiye’de bilişim alanında kritik altyapılara örnekler

Bu alanda Türkiye’de yapılan çalışmalara bakıldığında Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı; siber ortamı oluşturan bilgi sistemlerinin saldırılarından korunması, bu ortamda işlenen bilgilerin gizliliğinin sağlanması, bütünlüğünün ve erişilebilirliğinin korunması, siber güvenlik olaylarının saldırı ve tespiti bunlara karşı müdahale mekanizmaları tespit edilerek, sistemlerin siber güvenlik olayı öncesindeki durumlarına döndürülmesi açısından önemli bir adım olarak nitelendirilebilir.

Siber tehditler artık bilgisayar sistemlerine verdikleri zararla yalnızca sızma, sistemlerden bilgi çalma ve sistemlere yanlış bilgi yerleştirme gibi küçük etkilerle sınırlı değildir. Gerçekleştirilen saldırılar bir ülkenin bilgisayar, enerji, altyapı, ulaşım ve askeri komuta kontrol sistemleri gibi kritik yapılarına zarar verdiği ölçüde asimetrik bir savaş türü olarak karşımıza çıkmaktadır.

Bu nedenle siber tehditlerin dünyanın en önemli unsurlarından biri olacağı düşüncesi, gelecek yıllardaki tehditler tüm dünya tarafından kabul görmeye başlamıştır. Türkiye'nin stratejik planına göre siber güvenlik politikalarının özü; Siber ortamı oluşturan bilgi sistemlerini saldırılara karşı korumak, gizliliği, bütünlüğü ve erişilebilirliği güvence altına almak, bu ortamda işlenen bilgilere yönelik saldırıların algılanmasını sağlamak, yapılan bu algılamalara karşı mekanizmaları geliştirmek ve ardından sistemlerin siber saldırıdan önceki işler duruma döndürmektir. Dolayısıyla ülkenin siber güvenliğe yaklaşımının bilgi güvenliğinin ötesinde bir

güvenlik algısına sahip olduğu söylenebilir. ABD'nin ve diğer ülkelerin de siber güvenliğe "Bilgi Güvenliği" olarak yaklaştığı görülmektedir [11-13].



**Şekil 1.3:** Güvenlik değerlendirme

Hükümetler, siber saldırıları ve olayları, eyalet ve yerel yönetimler, özel sektör ve kamunun koordineli, odaklanmış çabalarıyla üstesinden gelinebilecek stratejik zorluklar olarak ele almaktadır. İngiltere'ye göre siber güvenlik; hem UK'nin siber uzaydaki çıkarlarının korunmasını hem de siber alanın sunduğu birçok fırsattan yararlanarak daha geniş İngiliz güvenlik politikasının oluşturulmasını kapsamaktadır. Avrupa Birliği (AB) siber güvenliğin dört farklı boyutla ilgilenir: bu boyutlar bilgi güvenliği, siber suç, siber casusluk ve siber savaş olarak nitelendirilebilir. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency-ENISA), siber güvenlik stratejisi eylem planlarına katkıda bulunan bir kuruluş olarak karşımıza çıkmaktadır. Bu kuruluş tarafından önerilen stratejik eylem planları: siber güvenliğe yönelik tavsiyelerden, politika oluşturmayı ve uygulamayı destekleyen faaliyetlerden ve AB genelindeki pratik faaliyetlerden oluşmaktadır [1, 2, 5-9].

ENISA ve ITU tarafından ülkelerin siber güvenlik strateji ve politikalarına yönelik çeşitli eylem planları ve kılavuzlar hazırlanmış; siber güvenlik stratejilerini karşılaştırmalı olarak incelemek için belirlenen ana ve alt boyutların kullanılmasına karar verilmiştir [1-3, 5-7, 10-16].

## 2. KAVRAMSAL ÇERÇEVE

### 2.1. ÜLKELERİN SİBER GÜVENLİK POLİTİKALARININ DEĞERLENDİRİLMESİ VE İLGİLİ ÇALIŞMALAR

Bilgi ve iletişim teknolojileri günümüzde yaşamın her alanında büyük kolaylık sağlamaktadır. Her alanda günden güne gelişen teknoloji, sağlamış olduğu kolaylığın yanında bir takım sorunlar da meydana getirmektedir. Hayatı kolaylaştıran teknolojik cihazlarda, sistemlerde ve altyapılarda meydana gelen sorunların başında gelen siber saldırılar, siber savaşın zamanla şiddetini artıracaklarını kanıtlamakta ve 21. yüzyılda siber uzayın güvenliğini sağlamanın kritik önemini ortaya koymaktadır [17].

Bu açıdan bakıldığında, ülkelerin en büyük sorunlarından olan siber savunma problemi; siber ortamı, kurumları, kuruluşları, sistemi ve kullanıcılara ait varlıkları korumak için, araçlar, yazılımlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitimler ve uygulamalar gibi açılardan ele alınmak zorundadır.

Nitekim, 2009 yılının Haziran ayında UK Kabine Ofisi ekibince düzenlenen “Birleşik Krallık'ın Siber Güvenlik Stratejisi” raporunda geçen: “Tıpkı 19. yüzyılda denizleri ulusal güvenliğimiz için koruma altına almak ve 20. yüzyılda havayı güvence altına almak zorunda kaldığımız gibi ulusal güvenlik ve refah, 21. yüzyılda siber uzaydaki avantajımızı da güvence altına almalıyız” ifadeleri siber uzayın önemini tam olarak anlatmaktadır.

Teknolojinin artması ve saldırı yöntemlerinin karmaşıklaşmasıyla birlikte, siber saldırıların eğilimi, küçük ölçekli sızma saldırılardan çıkarak bankacılık ve finansal sistemlere yönelik saldırılara, kritik altyapılara gerçekleşen yüksek düzeyde organize edilmiş devlet destekli saldırılara dönüşmüştür [18-20]. Güvenlik firmalarının yapmış olduğu araştırmalar, siber saldırıların çok büyük kısmının kurumsal/hükümet sistemlerini hedeflediğini; siber güvenlik stratejilerinin gelişimi, basit siber saldırılar eğiliminin devlet destekli büyük çaplı saldırılara kaymasıyla 2008'den sonra yavaş yavaş hız kazandığını göstermektedir.

Bu alanda çalışma yapan ilk ülkelerden olan ABD, siber saldırıların çok yaygın olmadığı 2003 yılında ilk strateji taslağını yayınlamıştır. Ancak genel olarak bakıldığında zaman ülkelerin çoğunun siber güvenlik stratejilerini 2011'de yayınladığı görülmektedir. Sürekli değişen siber tehdit yelpazesi, siber güvenlik stratejisinin ortaya çıkan tehditleri ve ilgili karşı önlemleri kapsayacak şekilde güncellenmesini zorunlu kılmıştır. Özellikle UK, ABD, Hollanda, Çekya

ve Estonya gibi ülkeler bu bilinçle birlikte stratejilerini geliştirerek sonraki versiyonlarını da yayınlamışlardır [60]. Tablo 2.1’de siber güvenlik seviyeleri açısından ülkelere yönelik bir değerlendirmeye yer verilmiştir.

**Tablo 2.1:** Yüksek siber güvenlik seviyelerine sahip gelişmiş ülkeler sıralaması [28]

| SIRALAMA | ÜLKE                                 |
|----------|--------------------------------------|
| 1        | Amerike Birleşik Devletleri          |
| 2        | Kanada                               |
| 3        | Avustralya                           |
| 4        | Yeni Zelanda                         |
| 5        | Estonya, Japonya, İngiltere, Almanya |
| 6        | Avusturya, İsrail, Hollanda          |
| 8        | Finlandiya                           |
| 9        | Fransa, İspanya                      |
| 12       | Çek Cumhuriyeti                      |

İş dünyasının önde gelen firmaları ve hükümet yetkililerine göre, bugün siber saldırılar tek başına fiziksel terörizmden çok daha fazla fiziksel ve finansal kayba neden olmaktadır. Saldırıları, son derece özelleştirilmiş yetkisiz giriş tekniklerini, son yöntemleri/araçları kullanmakta ve askeri, siyasi veya ekonomik istihbarat gibi yüksek oranda değerli ulusal bilgileri toplamayı amaçlamaktadır.

Özellikle 2007 yılında Estonya’nın ağ altyapı sistemlerine yönelik saldırılar, 2008 yılında Gürcistan ile Rusya arasında yaşanan ve 2008 yılında siber savaşa dönüşen fiziki savaş ve 2010 yılında İran’ın nükleer programına “Stuxnet” solucanı üzerinden yapılan saldırı başta olmak üzere geçmişte öne çıkan siber saldırılar, birçok ülkenin bu alanın kritikliğini fark etmesini sağlamıştır. Bu saldırılara bakıldığında zaman, bilgi ve iletişim teknolojilerinin hemen her alanda kullanıldığını, her sistemin altyapısında mevcut olduğunu ve bu alanlarda ulusal bilgi ve teknoloji altyapılarının siber saldırılara karşı son derece savunmasız hale getirdiğini göstermektedir.

2013’te Ulusal Güvenlik Ajansı (National Security Agency-NSA)’nın küresel internet iletişiminde toplu gözlemler sonucunda yaptığı açıklamalar neticesinde, birçok ülke ulusal yapıdaki önemli dijital verilerini korumak zorunda kalmış ve vatandaşlarının dijital dünyadaki haklarını koruma ve gözetme konusunda temkinli hale gelmiştir [21-23].

Bu bölümde ülkelerin siber savunma politikalarına yönelik yapmış oldukları çalışmalara yer verilmiştir. İspanya, Kanada, Japonya ve Avustralya, ABD ve Almanya’dan sonra dünyada en yüksek BİT kullanımına ve siber suç oranına sahip oldukları için seçilmiştir ve bu

ülkelerdeki çalışmalara yönelik yapılacak analizler, Türkiye’de siber suçlarla mücadele için potansiyel çalışmalarda güvenli yaklaşımları ortaya çıkarabilecektir.

UK, ABD, Çekya ve Estonya, ilk siber güvenlikle ilgili strateji taslağını düzenleyen ülkelerin başında gelmektedir. Hollanda, sivil siber güvenlik ve askeri siber savunma şeklinde iki ayrı güvenlik stratejisi çizmiştir. Finlandiya ve İsrail birçok güvenlik araştırmacısına göre siber mükemmelliğin başlıca örneği olarak görülmektedir. Malezya ise Asya Ülkeleri arasında siber güvenlikle ilgili en güçlü ülke olarak görülmektedir [32].

Hindistan ve İran son derece yüksek siber suç oranlarına sahip ülkeler arasındadır. Bu nedenle bu ülkelerin stratejilerini oluşturmak için, siber uzayı çeşitli tehditlere ve saldırılara karşı korumak için önemli çalışmalar gerçekleştirildiği görülmektedir. Bu durumlar ayrıca federal düzeyde siber yeteneğin oluşturulmasını ve Ulusal Siber Güvenlik Stratejisi (National Cyber Security Strategy-NCSS) gibi üst düzey bir eylem planının hazırlanmasını tetiklemiştir. Bu nedenlerden hareketle, Çekya, Hollanda, Finlandiya, Estonya, Fransa, Almanya, Türkiye ve İspanya gibi ana dili İngilizce olmayan ülkeler de İngilizce bir taslak politika yayınlamışlardır [24, 25]. Tablo 2.2’de gelişmekte olan ülkelere ait siber güvenlik seviyeleri sıralamasına yer verilmiştir.

**Tablo 2.2:** Yüksek siber güvenlik seviyelerine sahip gelişmekte olan ülkeler sıralaması [28]

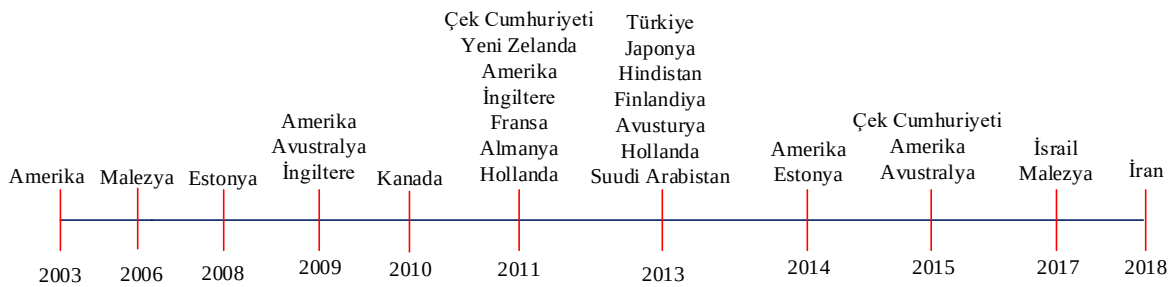
| SIRALAMA | ÜLKE      |
|----------|-----------|
| 1        | Malezya   |
| 2        | Hindistan |
| 3        | Türkiye   |
| 4        | İran      |

Yukarıda bahsedilen siber güvenlik stratejilerinin uluslararası değerlendirmesini yapmak için faydalı olacağı düşünülen bazı metrikler aşağıdaki gibidir:

- Siber güvenlik stratejisi veya politikasının yayınlandığı yıl
- Stratejilerin ana hatlarıyla belirtilen amaçları
- Siber uzay ve siber güvenlik gibi temel anahtar terimlerin anlaşılması
- Ulusal siber güvenliğe verilen öncelik düzeyi
- Ülkenin siber tehdit algısı
- Siber güvenlik durumunu sürdürmekten sorumlu kuruluşlar ve kamu aktörleri
- Stratejide listelenen kritik sektörler ve altyapı

- Siber erken uyarı sistemleri, tehdit bilgi paylaşımı yaklaşımları, Bilgisayar Acil Müdahale Ekipleri (Computer Emergency Response Team-CERTS) vb. kuruluşların mevcut olup olmadığı
- Yasal önlemler
- Ülkenin araştırma ve geliştirme (AR-GE), siber işgücü geliştirme, siber farkındalık vb. çabaları
- Siber güvenlik için uluslararası işbirlikleri.

Siber güvenlik kavramı temelinde bu alandaki son gelişmeler göz önünde bulundurulduğunda, ulusların siber uzay alanında hem savunma hem de saldırı önlemleri bakımından kıyasıya bir rekabet içinde olduklarını söylemek doğaldır. Bu nedenle ülkelerin, her geçen gün kamuoyunda güvenlik bilincini artırmak için savunma ve taarruz kabiliyetine sahip siber birimler kurması, eğitim ve tatbikat faaliyetleri gerçekleştirmesi, sempozyumlar, çalıştaylar ve konferanslar düzenlemesi gerekmektedir. Bununla birlikte, ülkenin siber tehdit ortamı, sosyo-politik koşulları, güvenlik eğilimleri, gelenekleri, siber farkındalık düzeyi vb. durumları analiz edildiğinde seçilen ülkelerin siber güvenlik yaklaşımlarında önemli farklılıklar olduğu gözlemlenmiştir [26-29]. Şekil 2.1’de ülkelerin siber güvenlik politika yayımlama zaman çizelgesi sunulmuştur.



**Şekil 2.1:** Ülkelerin siber güvenlik politika yayımlama zaman çizelgesi [28]

Ülkelerin siber güvenlik politikalarına bakıldığı zaman ele alınması gereken önemli stratejik hedeflerin:

- Güvenli ve esnek bir siber uzay oluşturmak ve bu istikrarı sürdürmek,
- Kritik ulusal siber varlıkları ve altyapıları güvence altına almak,
- Siber güvenlik düzenleyici, yasal ve güvence çerçevesini tanımlamak,

- Vatandaşlar, devlet yetkilileri, Bilgi ve Teknoloji (BT) uzmanları arasında siber farkındalığı artırmak,
  - Siber güvenlik olayı algılama ve müdahale ekibini ve yeteneklerini geliştirmek,
  - Yerli siber güvenlik teknolojilerini geliştirmek,
  - Kamu-özel sektör işbirliğini teşvik etmek,
- olduğu sonucuna varılmaktadır.

Siber güvenlik stratejileri, ulusal güvenlik veya savunma stratejilerinin bir parçasıdır ve siber güvenliğin bir bütün olarak toplum üzerindeki her şeyi kapsayan etkisi nedeniyle ülkelerin ve diğer birçok kurumun stratejileriyle bağlantılıdır.

Aşağıda bazı Avrupa ve Asya ülkelerinin siber güvenlik stratejilerine ve siber politika hedeflerinin uygulamalarına, önlemlerine genel bir bakış sağlanmıştır. Ayrıca Türkiye'nin bu anlamda gerçekleştirdiği çalışmalar incelenmiş ve güvenlik değerlendirmesi verilmiştir [30, 31].

Genel olarak ulusal siber güvenlik stratejilerine ilişkin bu genel bakış, incelenilen ülkelerde siber güvenlik stratejilerinin entegre ve kapsamlı hale geldiğini ortaya koymaktadır. Ülkelere ait stratejiler, siber güvenliği bütüncül bir yaklaşımla ele almakta ve siber güvenliğin ekonomik, sosyal, yasal, kanun yaptırımı, askeri ve istihbaratla ilgili yönlerini kapsamaktadır.

Slovakya ve Çekya'da uygulanan strateji ve politikalar daha esnek bir yaklaşımı desteklemekte ve siber güvenlik politikasının ekonomik ve kişisel (bireysel) boyutlarını vurgulamaktadır. Ayrıca Çekya, Slovakya ve Macaristan, sivil kurumların siber güvenliği sağlamaktan sorumlu olduğu bir grup ülke olarak değerlendirilebilir. Bu bağlamda bu ülkelerde siber güvenlik sivil odaklı olarak nitelendirilebilir. Estonya, Litvanya, Letonya ve Polonya'da askeri kurumların siber güvenlik politikalarını koordine etme olduğu ve uygulama konusunda daha aktif rol aldıkları görülmektedir [30, 31].

Siber uzay savunması analiz edildiği zaman, bir güvenlik yaklaşımında ülkeleri varoluşsal olarak tehdit eden kritik altyapıların savunmasının ne derece önemli olduğu görülmektedir. Bu durum kritik altyapıların dijital dünya ile iç içe olmasından kaynaklanmaktadır. Bu ağlar kolektif bir yapı olarak tanımlanmaktadır ve zararlarının ulusal güvenliğe bir tehdit oluşturacağından farkına varılıp genellikle ilk başta güvenliğinin sağlanmaya çalışıldığı görülmektedir.

Ekonomik açıdan değerlendirildiği zaman özel sektör kuruluşlarının da bilgisayar korsanlarının vereceği zarardan büyük oranda korktuğu görülmektedir. Fikri mülkiyet hakkı

sahiplerinin veya bireysel kullanıcıların da dosya paylaşımının hak ve gelirlerini tehlikeye atacağına dair endişeleri bulunmaktadır. Bu açıdan değerlendirme yapıldığı zaman kişisel güvenliği ön planda tutan siber anlayıştan kaynaklanan “bireysel bir siber yaklaşım” olarak değil, ticari, toplumsal ve politik nedenlerden ötürü “ulusal bir yaklaşım” olarak ele alınması gerektiği hususu doğmaktadır [32-35].

Kritik altyapıların güvenliğini sağlamak gerektiği ve altyapının çöküşünün sonuçlarının, toplum, rejim ve ekonomi anlamında etkiye sahip olacağı düşüncesiyle yola çıkan; dört Orta Avrupa ülkesi olan Çekya, Macaristan, Polonya ve Slovakya arasında bölgesel ortaklık olan “Vişegrad Ülkeleri” ve Baltık Devletleri gerçekleştirdikleri siber güvenlik çalışmalarıyla çeşitli referans nesnelere ilişkin teorik bir bakış açısını sağlamak için, devletlerin kendileri tarafından tanımlanan referans nesnelerinin bir analizinin olması gerektiğini savunmuşlardır. Bu ülkelerin tamamı, siber ve ulusal güvenlik sektörleri arasında bir bağlantı olduğunu kabul etmektedir ve bilgi ve iletişim sisteminin veya kritik altyapının yok edilmesi gibi siber güvenlik konularının ulusal güvenliğe zarar verebileceğinin, vatandaşların hayatlarını çeşitli şekillerde etkileyebileceğinin ve varlıkları ve devleti tehdit edebileceğinin farkındadır. Bununla birlikte, siber alanlarını yoğun bir şekilde savunmaya yönelik güçlü bir ihtiyacı dile getiren Estonya, Polonya, Letonya, Litvanya ve Çekya gibi ülkeler, stratejik belgelerinde de sundukları gibi, daha kapsamlı ve daha net vizyonlar da sunmaktadır. Örneğin, Litvanya'nın ulusal güvenlik stratejisi, ulusal güvenlik politikasının temel hedefi olarak bilgi, ekonomik ve sosyal altyapının güvenliğini sağlamanın önemini 2012 yılında yayımladığı “Litvanya Cumhuriyeti Ulusal Güvenlik Stratejisi” ile vurgulamaktadır. Çekya'nın ulusal siber güvenlik stratejisi, 2011 yılında yayımladıkları “2011-2015 yılları için Çek Cumhuriyeti Siber Güvenlik Stratejisi” ile esas alınmış, ekonomik ve sosyal çıkarları için gerekli olan bilgi altyapısının korunmasına öncelik vermiştir. Ayrıca internet kullanıcılarının haklarının korunmasının da önemine büyük bir oranda odaklanmışlardır. Bununla birlikte, Çekya'nın ulusal güvenlik stratejisi, kritik altyapı ve siber uzaydan gelen güvenlik açıkları hakkında ulusal siber güvenlik stratejisinden daha kapsamlı bir içerik sunmaktadır [28-30].

Siber uzaylarını güvenlik altına almak isteyen ülkelerin, ulusal güvenliğin kilit koşulu olarak kritik altyapının güvenliğini önceliklendirmesi daha olası ve zorunludur. Ulusal güvenlik, referans nesne olarak kritik altyapıya bağlı bir yapıdır. Güvenlik ve savunma gerektiren nesneleri belirleme yetkisine sahip aktörler, güvenlik adına olağanüstü araçlar kullanma hakkını sahip olmalı ve bir koordinatör olarak görev yapmalıdırlar. Polonya'nın 2015 yılında yayımladığı “Polonya Cumhuriyeti Siber Güvenlik Doktrini”, kritik altyapının önemini

ve siber güvenlik ile ülkenin ekonomik gelişimi ve askeri alanda etkin bir şekilde faaliyet gösterme yeteneği dâhil olmak üzere düzgün işleyişi arasında doğrudan bir ilişki olduğunu vurgulamaktadır. Ayrıca Polonya, 2012 yılında yayımladığı “Polonya Cumhuriyeti Ulusal Güvenlik Stratejisi” ile siber uzayda potansiyel rakipleri caydırmak için sadece savunma amaçlı değil aynı zamanda saldırgan bir politika benimseyerek siber yetenekler geliştirmeye odaklı tek Vişegrad ülkesi değerlendirilebilir. Bu nedenle, Polonya'nın yaklaşımı, siber tehditleri belirleme ve bunlara karşı savunma süreci ne kadar belirginleşirse, o kadar askerileştiğini ortaya koymaktadır. Öte yandan, Macaristan ve Slovakya gibi ülkeler de politikalarında temel referans olarak kritik dijital altyapıyı ele almışlardır. Bununla birlikte, bu ülkeler diğer kritik altyapılara yönelik olası saldırıları ulusal beka için bir tehdit olarak görmemektedir, çünkü bu iki ülkede siber güvenliğin birkaç ulusal güvenlik sektöründen sadece biri olduğu düşünülmektedir. Macaristan ve Slovakya temel olarak bilgi güvenliğine odaklanmaktadır. Slovakya'nın bilgi güvenliği stratejisinin hedeflerinin, insan haklarını ve özgürlüğünü korumaya, bilgi güvenliği yönetimini geliştirmeye yönelik olduğu ve bu amaçla devletin kritik altyapısını desteklemek için devlet bilgi ve iletişim altyapılarını savunmaya 2008 yılında yayımladığı “Slovak Cumhuriyeti'nde Ulusal Bilgi Güvenliği Stratejisi” ile odaklandığı görülmektedir [30-35].

Macaristan'ın siber güvenlik stratejisindeki referans alınan kavramların daha da bilinçsiz olduğu görülmektedir. 2013 yılında yayımladıkları “Macaristan Ulusal Siber Güvenlik Stratejisi Üzerine Hükümet Kararı” ile ele alınan strateji, yalnızca ulusal veri varlıklarının korunmasından ve siber uzayla bağlantılı kritik altyapılarının bölümlerinin operasyonel güvenliğinden bahsetmektedir. Ne Slovakya ne de Macaristan, siber güvenlik kapsamında öncelikle korunması gereken belirli bir referans nesnesi tanımlamamaktadır; sonuç olarak, her iki ülkenin de siber güvenliğe sivil bir yaklaşımı olduğu ve yetersizliği görülmektedir.

Siber tehditlerin kişisel amaçlarla yola çıkan saldırılar tarafından maddi kazanç elde etmek amacıyla geleceği gibi çoğunlukla yabancı hükümetler veya devlet dışı aktörler gibi kötü niyetli ajanların finansal, enerji veya kamu güvenliği sistemlerine erişim sağlamaya çalıştığında ortaya çıktığı görülmektedir. Bu siber saldırın oluşturacağı hasarların da bu şekilde algılanması ve sunulması gerektiği, yoğun güvenlik önlemlerine yol açtığı unutulmamalıdır; bu doğrultuda önlemlerin de bir o kadar yoğun alınması gerektiğini ortaya çıkmaktadır [35-38].

Sonuç olarak, ulusal güvenlik söyleminin hâkim olduğu ülkelerde siber saldırı tehdidi öncelikli kabul edilmeli ve siber güvenliğe, politikalara, alınacak önlemlere askeri ve devletlerarası bir yaklaşımla bakılması söz konusu olmaktadır.

Ancak siber ve ulusal güvenliğe yönelik tehditler yalnızca dış kaynaklardan kaynaklanmamaktadır. Bu nedenle, siber saldırılar sistematik tehditlerden de kaynaklanabilmektedir. Bilgisayarların ve bilgi sistemlerinin kendileri veya içinde bulundukları fiziksel ve insan ortamları istenmeyen tehlikeli durumlar (potansiyel veya fiilen) yaratmakta olmakla birlikte bu tehditlerin öngörülemezliğinden kaynaklanan sorunlar da mevcuttur. Bu nedenden ötürü siber saldırıları belirli bir sektör için risk olarak algılayan ülkeler, siber sorunları ulusal güvenlik sorunları olarak tanımlamada daha yetersizdir [39-41].

Polonya, Letonya, Litvanya, Estonya ve Çekya, siber saldırılara karşı çok katmanlı bir yaklaşıma sahip ülkelerdir. Bu ülkelerin, ilk olarak ulusal güvenliklerine yönelik riskleri değerlendirdikleri ve devlet kurumlarına siber saldırıları önleme görevi verdikleri görülmektedir. İkinci olarak, ulusal güvenliklerinin ayrılmaz bileşenleri olan ekonomik, finansal ve özel sektörlerle yönelik siber bağlantılı sorunları tespit ettikleri görülmüştür. Siber saldırılara yönelik bu kapsamlı yaklaşımın, Estonya'nın siber güvenlik stratejisine de yansıdığı görülmektedir. Estonya, 2014 yılında yayımladığı “2014–2017 Estonya Siber Güvenlik Stratejisi” ile siber casuslukla mücadele etmek ve hem internete bağlı hem de kapalı ağları korumakla görevli, ek olarak güvenlik ve ekonomik çıkarlar hakkında bilgi toplamak amacıyla artan sayıda devlet aktörüne sahip olduklarını savunmuşlardır. Ulusal güvenlik, Polonya'nın siber güvenlik doktrinine de hâkim bir söylemdir. Polonya doktrininde tanımlanan siber tehditler, ulusal güvenlik ve siber suç için önemli olan telekomünikasyon sistemlerine yönelik saldırıları içermekte olup belirtilen belirli siber suçlar arasında siber şiddet, yıkıcı siber protestolar ve siber gösteriler, veri ve kimlik hırsızlığı ve özel bilgisayar korsanlığı yer almaktadır. Aynı yaklaşımların Litvanya ve Letonya'nın stratejik belgelerinde de yer aldığı görülmektedir. Örneğin, Litvanya'nın 2012 yılında yayımladığı “Letonya Cumhuriyeti Devlet Savunma Konsepti”nde devlet savunma konsepti, siber saldırıları terörizm ve organize suç faaliyetleri ile birlikte ulusal bir tehdit olarak gruplandırmaktadır.

Yukarıda bahsedilen dört ülkede de, siber saldırıların farklı sektörler ve genel olarak ulusal güvenlik üzerindeki potansiyel etkisinin kesin değerlendirmelerine dayanan kapsamlı bir siber güvenlik yaklaşımına sahip olduğu görülmektedir. Siber saldırıları temelde ulusal güvenliğe tehdit olarak algıladıklarından, bu ülkelerin askeri ve uluslararası bir yaklaşımla ele aldıkları değerlendirilebilir [42, 43].

Slovakya'nın 2015-2020 için güncellenmiş siber güvenlik konseptinin de karma bir siber güvenlik algısı sunduğu görülmektedir. Slovakya, siber güvenliğin Slovakya'nın münferit bir sorunu olarak ya da bir veya birkaç sektöre münferit bir konu olarak görülmemesi gerektiğini

ve küresel doğası gereği siber güvenliğin toplum çapında bir olgu olduğunu iddia etmektedir. Aynı zamanda Slovakya'nın siber tehditlerin yeterince acil bir sorun olarak görmemesi ve Slovak hukukunda açıkça veya geçerli bir şekilde ele almamasından ötürü ülkenin siber güvenlik politikasının temel sorununu olarak ortaya çıkmaktadır.

Çekya'nın stratejisi ise endüstriyel, askeri, siyasi vb. alanlarda siber casusluk, siber uzayda organize suç, hacktivizm, siyasi veya askeri amaçlı kasıtlı dezenformasyon ve siber terörizm gibi kavramlardan bahsetmektedir. Bu riskler, küresel siber uzayda Çek toplumunu henüz tehdit etmeyen tehlikeli eğilimler olarak görülmüştür. Çekya'nın stratejik belgelerinde hâkim olan güvenlik söylemi, temel olarak sistematik tehditlere ve “bilgisayar güvenliğine” atıfta bulunmaktadır. Bu bağlamda yayımlanan “Çek Cumhuriyeti Siber Güvenlik Stratejisi”nde, Çekya'nın siber güvenlik stratejisi, esas olarak hizmetlere erişimi güvence altına almak, veri bütünlüğünü korumak ve Çekya'nın siber alanlarının gizliliğini teşvik ederek güvenilir bir bilgi toplumu oluşturmak gibi konulara odaklanılmıştır.

Macaristan ise 2013 yılında yayımladığı “Macaristan Ulusal Siber Güvenlik Stratejisine İlişkin Hükümet Kararı”nda siber saldırıların suç unsuru olduğu vurgulanmış; Macaristan’da, bulut bilişim ve mobil internet gibi dinamik olarak gelişen yeni teknolojilerin, kritik bilgilerin ve kişisel verilerin yasa dışı edinilmesi gibi yeni güvenlik risklerinin sürekli ortaya çıkmasına yol açtığı iddia edilmiştir. Ancak Macaristan’ın siber güvenlik sorunlarını tehditlerle tanımlamaktan kaçındığı ve siber tehditleri siber sektör için riskler olarak adlandırmayı tercih ettikleri görülmüştür. Çekya, Slovakya ve Macaristan'da hâkim olan siber güvenlik anlayışında uluslararası ve politik bir yaklaşımla ele almaktan çok basit bir siber tehdit ve siber güvenlik problemi olarak tanımladıkları görülmektedir.

Siber tehdit kaynaklarının belirli ülkeler tarafından nasıl anlaşıldığına dair gerçekleştirilen analizler ile birçok ülkelerin siber uzayda çok sayıda aktör olduğunu kabul ettiği sonucuna götürmektedir. Ancak, yalnızca birkaç devlet bu aktörlerin doğası, amaçları ve yöntemleri arasında bir ayrım yapmaktadır. Örneğin Estonya'nın siber güvenlik stratejisi, ulusal siber güvenliğin, siber uzayda çeşitli beceri, hedef ve motivasyonlarla faaliyet gösteren aktörlerden etkilendiğini ve ulusal güvenlik ve ekonomik bilgi toplama amaçlı siber casusluğun arttığını iddia etmektedir ki nitekim bu iddia doğru bir yaklaşım olarak ele alınabilmektedir. Estonya'nın stratejisi aynı zamanda siber saldırılar yapabilen ve fiilen başlatabilen devletlerin sayısının arttığını da vurgulamaktadır. İç ve dış tehditler arasındaki bu ayrım Polonya doktrininde de yapılmıştır. Doktrin tarafından listelenen dış tehditler arasında siber krizlerin, siber çatışmaların, siber savaşların ve devletleri ve diğer birimleri içeren siber casusluğun yer

aldığı görülmektedir; siber uzaydan gelen tehditlerin, terörist ve siber uzaydaki saldırıları ideolojik, siyasi olabilecek uluslararası suç örgütlerini içerdiği de yer almaktadır.

Buna karşılık Litvanya ve Letonya, tam olarak siber saldırganları tanımlamamıştır, ancak stratejik politikalarında öncelikle komşu ülkeleri dış tehdit olarak tanımlamışlardır. Ayrıca hem Slovakya hem de Macaristan, siber tehditlerin kaynakları konusunda oldukça bulanık ve parçalı bir vizyona sahip ülkeler olarak karşımıza çıkmaktadır. Örneğin, Macaristan teknolojik güvenlik açıklarına, bunların nedenlerine ve sürece dâhil olan aktörlere ilişkin daha derin bir analiz yapmadan yalnızca devlet ekonomisinin düzgün işleyişi üzerindeki etkilerine odaklanmıştır. Macaristan'ın siber güvenlik stratejisi, dış etkenlerin verdiği zararın yanı sıra, siber uzayı oluşturan bilgi ve iletişim sistemlerinin operasyonel güvenliğinin yeterince düzenlenmemesinin de bir risk oluşturduğunu belirtmektedir. Siber tehditlerin kaynaklarına yönelik dar bir yaklaşımın Çekya'da da var olduğu görülmektedir. “Çek Cumhuriyeti Ulusal Güvenlik Stratejisi”, çok çeşitli potansiyel siber zorlukları tanımlamıştır; ancak, kişisel veya hassas verileri çalan bilgisayar korsanların, teknolojik arızaların, botnet'lerin, DDoS/DoS (Hizmet Reddi) saldırılarının vb. temel suç veya teknolojik nitelikte olduğunu değerlendirmişlerdir.

Ayrıca Estonya, Polonya, Litvanya ve Letonya gibi ülkeler, dış ve iç siber aktörler arasında bir ayrım yapmaktadır. Bunların yanı sıra, siber tehditlerin suç unsuruna vurgu yapan ülkeler, bunları siber uzayın iç zorlukları ve sınırlamaları olarak görmektedir. İncelenen ülkelerin neredeyse tamamının stratejik belgelerinde siber tehditlerin iç ve dış kaynakları arasında bir ayrım yapması dikkat çekicidir. Ancak politikalarını sivil odaklı olarak tanımlayan ülkelerin ve Doğu Avrupa Ülkelerinin siber güvenlik politikalarında bu ayrımı detaylandırmadığı ve güvenlik ortamlarında en yaygın ve daha çok olası iç tehditlere odaklandığı görülmektedir.

Dört Vişegrad ülkesinin ve üç Baltık Devleti'nin siber güvenlik politikalarının niteliksel analizi, bu ülkelerin her birinin siber güvenlik konularını ele almak için siber güvenlik stratejilerine ve ilgili yasalara sahip olduğunu göstermektedir. İncelenen stratejilerin tamamında üst düzey ulusal güvenlik veya savunma stratejilerine atıfta bulunulduğu ve önemli farklılıklar olmasına rağmen genellikle bu hususta mevzuatların geliştirdiği görülmektedir. Yayımlanan politikalarda, farklı siber uzay varlıklar tanımlanmış ve bu varlıkların oluşturduğu farklı potansiyel tehditler de ele alınmaktadır. Çoğu ulusal siber güvenlik stratejisinde, kritik altyapıya yönelik tehditler ve siber suçlar önemli bir rol oynamakta ve siber saldırıların neden olduğu artan ekonomik zarar gösterilmektedir.

Ancak, ülkeler arasında siber güvenlik politikalarında bazı farklılıklar vardır. Siber güvenlik konularını militarize eden ve askeri bir açıdan ele alan ülkeler kategorisine Polonya, Estonya, Litvanya ve bir dereceye kadar Letonya dâhil edilebilir. Siber güvenlik söylemini militarize etmiş olan bu ülkeler, belirli referans nesnelerini belirlemekte ve bu nesnelerin savunmasını ulusal öncelikler olarak ifade etmektedir. Bu eğilim, siber güvenliği en yüksek ulusal güvenlik düzeyine yükseltmiş ve hükümet bilgi kaynaklarının korunmasına odaklanmıştır. Polonya, Estonya ve Litvanya, siber güvenlik sorunlarını devletin düzgün işleyişine yönelik tehditler olarak belirleme ve yabancı devletlerden gelen saldırıları bu tür tehditlerin en tehlikeli kaynakları olarak belirleme eğilimindedir. Sonuç olarak, bu devletlerde siber tehditlere yanıt verme sorumluluğu askeri ve savunma kurumlarına devredilmektedir. Çekya, Slovakya ve Macaristan siber güvenliği sağlamak için sivil bir yaklaşım belirlemiştir. Ele aldıkları tutum ve önlemler dağınıktır ve esas olarak devletin ekonomik sisteminin ve özel mülkiyetin düzgün işleyişi ile ilgilidir [30-33, 44]. Bu ülkelerin analizi ile elde edilen sonuçlar, siber güvenlik yaklaşımlarının sivil veya askeri olarak sınıflandırıldığını göstermektedir.

Uluslararası siber güvenlik politikaların analiz edilmesi ve değerlendirilmesi için Asya ülkelerinin de politikalarına bakmak faydalı olacaktır. Endonezya Hükümeti, siber uzayı siber suç tehdidinden korumak için bir dizi çalışma yürütmüştür. Hükümet'in siber uzayda bilgi güvenliğini korumaya yönelik çalışmalarından en önemlisinin, "Telekomünikasyon Yasasını ve Bilgi ve Elektronik İşlemler Yasası"nı yayınlamaları olduğu değerlendirilebilir. Daha sonra, bilgi güvenliği ile ilgili düzenlemeleri ve politikaları formüle etmenin temeli olarak değerlendirmiş; ana sorumluluğu siber saldırıları önlemek ve acil bir strateji oluşturmak olan Ulusal Siber ve Şifreleme Ajansı'nı kurmuşlardır. Kurulan ajans ile ayrıca ülkenin siber tehditlere karşı savunmasını güçlendirmek istemişler ve siber güvenlik konusunda kamuoyu bilincini artırmak için çalışmalar yürütmeyi amaçlamışlardır. Kişisel Verilerin Korunması (KVK) ve mahremiyet konusunun da öneminin bilincinde olarak, "Bilgi ve Elektronik İşlemler Yasası" kapsamında bir kılavuz olan "Elektronik Sistemlerde Kişisel Verilerin Korunması" yönetmeliği yayınlanmıştır. Ayrıca, KVK ile ilgili yeni bir kanun olan ve Endonezya'da özellikle kişisel verilerin korunmasıyla ilgilenen ilk kapsamlı yasa tasarısı "KVK Kanun Tasarısı" çalışmaları yapılmıştır.

Malezya, siber ortamla ilgili birçok mevzuata sahiptir. Ancak, siber tehditlerle mücadele için kullanılan yasa bilgisayarların kötüye kullanılmasıyla ilgili suçları önlemek ve mevcut ceza yasalarını tamamlamak için oluşturulan "Bilgisayar Suçları Yasası"dır. Kişisel verilerin

korunması sorunları ve kişisel verilerin kötüye kullanılmasını önlemek için “Kişisel Verileri Koruma Yasası” kullanılmaktadır [32].

2012'de Filipinler hükümeti, siber suçları tanımlayan “Siber Suçları Önleme Yasası”nı hazırlamışlardır. Bu kanun, sadece siber suç ve cezanın bir özelliğini tanımlamakla kalmamış, aynı zamanda bir kanun uygulamasına da rehberlik etmiştir. Bu çalışmanın ardından 2018 yılında hükümet, siber suçları soruşturma ve kovuşturma yetkisine sahip olan ve uluslararası bir işbirliğini kolaylaştıran “Filipin Siber Suç Ofisi”ni kurmuştur. Filipinler, bu çalışmalar kapsamında ayrıca daha kapsamlı ve katı bir gizlilik yasası olan “2012 Veri Gizliliği Yasası”nı da kabul etmiştir. Bu yasa, yenilik ve büyümeyi teşvik etmek için serbest bilgi akışını sağlarken bireylerin mahremiyetini korumakta; kişisel verilerin toplanmasına, kaydedilmesine, düzenlenmesine, saklanmasına, güncellenmesine veya değiştirilmesine, alınmasına, silinmesine veya imha edilmesine yönelik durumları düzenlemektedir. “Filipinler'in Ulusal Gizlilik Komisyonu” aracılığıyla veri koruması için belirlenen uluslararası standartlara uyulmasını sağlamaktadır.

Singapur, siber güvenlik tehditlerini diğer Asya ülkelerine göre daha ciddiye almaktadır. Bu algı ile ulus için siber güvenliğin tüm yönlerini denetlemek ve koordine etmek için merkezi kurum olarak nitelendirdikleri “Singapur Siber Güvenlik Ajansı”nı kurmuşlardır. Singapur'daki bilgisayar suçlarıyla ilgili ana mevzuatın, yayınlanan “Bilgisayarı Kötüye Kullanma Yasası” olduğu değerlendirilebilir. Söz konusu yasa ile, yetkisiz erişimin engellenmesinde, verilerin değiştirilmesinde ve diğer bilgisayar suçlarını önlemede öncü olmak için 1993 yılında çıkarılmıştır. Ayrıca bu yasa, suç tanımındaki değişikliklere ayak uydurmak için 1994 ve 2013 yılları arasında iki kez değiştirilmiştir. 2013 yılında, siber güvenlik önlemlerini içerecek şekilde değiştirilmiş ve “Bilgisayarın Kötüye Kullanımı ve Siber Güvenlik Yasası (Computer Misuse and Cybersecurity Act-CMCA)” olarak yeniden adlandırılmıştır. 2017'de Singapur Parlamentosu, mevcut Bilgisayar Kötüye Kullanımı ve Siber Güvenlik Yasası'nda yapılan değişiklikleri onaylamıştır. Yapılan değişiklikler ile siber suçun artan ölçeğinin belirlemek ve ulusötesi doğası ile siber suçluların gelişen taktiklerini ele almak üzere tasarlanmıştır. Kişisel veriler ve mahremiyet konularıyla ilgili olarak ise, “2012 Kişisel Verilerin Korunması Kanunu” yürürlüğe girmiştir ve bu kanun kişisel verilerin toplanması, kullanılması, ifşası ve tutulmasına ilişkin kuralları içermektedir.

Tayland Hükümeti, son yıllarda altyapıyı geliştirmeyi, yeniliği hızlandırmayı ve ülke ekonomisini dijitalle dayalı bir ekonomiye dönüştürmeyi amaçlayan bir dizi stratejiyle Tayland'ın bilgi ve iletişim teknolojisi sektörünün ilerletilmesini amaçlamaktadır. Bu

doğrultudaki çalışmalara ek olarak, ülkenin kabinesi, 2016 yılında e-ticaret yoluyla mal ve hizmet ticaretini kolaylaştırarak Tayland ekonomisini bir üst seviyeye taşımayı amaçlayan “Tayland Ekonomi 4.0” adlı bir projeyi resmi olarak onaylamıştır. “Dijital Ekonomi ve Toplum Bakanlığı” tarafından, dijital ekonominin gelişimini desteklemek için sekiz maddelik mevzuatın kabul edilmesi önerilmiştir. Bu sekiz maddeden en tartışılabilir, hükümetin web sitelerini kapatmasına ve yasa dışı veya hassas olduğu düşünülen herhangi bir içeriği kaldırmayan internet servis sağlayıcılarını cezalandırmasına izin veren “Bilgisayarla İlgili Suç Yasası”nda yapılan değişikliktir. Kişisel verilerin korunmasına gelince, Tayland'ın 2017 yılına kadar veri koruma veya gizliliği düzenleyen herhangi bir genel kanununun bulunmadığı görülmektedir. Bununla birlikte, “Tayland Krallığı Anayasası” ve “Mali Kurumlar Yasası ve Ulusal Sağlık Hizmetleri Yasası” gibi çalışmalarla bazı sektörlerde izinsiz toplama, işleme ve ifşaya karşı belirli bir düzeyde koruma sağlamayı amaçlamıştır. Bu anlamda oluşturulan “Kişisel Bilgilerin Korunması Kanunu” çalışmaları, veri sahibinin rızası olmaksızın her türlü kişisel verinin toplanmasını, kullanılmasını, ifşa edilmesini ve değiştirilmesini kısıtlayarak kişisel verilerin korunmasını sağlamaya çalışmaktadır. Yapılan son çalışmalar ile bu kuralların ihlal edilmesi durumunda hem oluşacak cezai yaptırımların belirlenmesi ve bir “Kişisel Verilerin Korunması Komisyonu”nun kurulması gerektiği bilincinin oluştuğu görülmektedir.

Vietnam, 2005 yılında elektronik işlemler hakkında bir yasa geliştirmiştir ve bu kapsamda yeni bir “Siber Bilgi Güvenliği Yasası”nı yürürlüğe koymuştur. Yasa, 19 Kasım 2015'te Vietnam Sosyalist Cumhuriyeti Ulusal Meclisi tarafından kabul edilmiş; 1 Temmuz 2016'dan itibaren yürürlüğe girmiştir. Bu çalışmayı Vietnam'da söz konusu tarihe kadar yayınlanan ilk kapsamlı yasa olarak değerlendirmek mümkündür. Yasa ile ele alınan temel amaç, internet ağının hem güvenliğini hem de bütünlüğünü ele almak ve ağ ortamındaki kişisel bilgilerin korunmasını sağlamaktır. Yürürlüğe giren kanun, dijital bilgileri sınıflandırmak ve kamu kuruluşlarının bu tür verileri korumak için izlemesi gereken adımları tanımlamak için bir sistem belirlemektedir. Ayrıca “İletişim ve Enformasyon Bakanlığı”nı ve “Vietnam Bilgisayar Acil Müdahale Ekibi”ni ülkenin siber suça karşı savaşında sorumlu oluşumlar olarak görevlendirmiştir.

Altı Asya ülkesinin siber güvenlik politikası ve mevzuatı gözden geçirildiğinde, Asya'daki çoğu ülkenin, dijital kullanıcıların sorumluluğunu belirledikleri, bu ortamlarda kötücül davranışların hukuki sorumluluklarını belirleyen yasalar oluşturdukları, siber suçla mücadele etmek ve oluşacak tehdit konularını ele almak için bazı mevzuat ve politika geliştirme çalışmalarını yaptıkları görülmektedir. Vatandaşlarının mahremiyetini sağlamak için yasalar ve

düzenlemeler sağlayarak kişisel verilerin korunmasına özen göstermek amaçlanmıştır. Ancak, her bir mevzuat ve politikanın gelişme düzeyi ve içeriği aynı yeterlilikle ele alınamamaktadır. Endonezya, Filipinler, Tayland ve Vietnam, bir hak sahibinin telif hakkı korumalarını bir bildirim sistemi aracılığıyla doğrudan uygulaması için yasal hükümler koymamakta, bunun yerine yasal işlem yoluyla veya yargı sistemi tarafından atıfta bulunulan telif hakkı yaptırımını işletmeye çalışmaktadır. İncelenen altı Asya ülkesinin hepsi de siber suçlarla ilgili bir tür mevzuata sahiptir. Ancak Endonezya, elektronik bilgi ve işlem yasasına dayanan veri koruma konusunda belirli bir siber güvenlik yasasına sahip değildir. Tayland ve Endonezya haricinde tüm ülkelerde veri korumaya ilişkin kanunlar mevcuttur. Tayland ve Endonezya'nın mahremiyet konusunda bir kanunu yoktur, bunun yerine farklı kanun ve kararnamelerle bu konuda ayrı kurallara sahiptir. Vietnam, hem güvenlik hem de veri korumayı tek bir siber bilgi güvenliği kanununda ele alan kapsamlı bir kanuna sahip olan tek ülkedir. “Malezya Kişisel Verileri Koruma Yasası”nı yalnızca hükümet tarafından işlenen verilerde değil ticari alanda da uygulamaktadır. Asya ülkeleri arasında ele alınması gereken önemli bir konu işbirliğidir, çünkü işbirliği ve bilgi paylaşımı gerçekten de siber güvenliğin sağlanmasında hayati bir önem taşımaktadır. Asya ülkeleri arasında siber olaylarla ilgili bilgi ve istihbaratın koordine edilmesi ve paylaşılması için kullanılacak bir bölgesel siber güvenlik koordinasyon platformunun kurulması ve bunun bölgesel politika gündemlerinden biri haline getirilmesi bölgesel alanda önemli bir adım olacaktır [32].

**Tablo 2.3:** Gerçekleşen büyük siber olaylara örnekler [23]

| S.N | YIL       | SİBER OLAY                                                                     |
|-----|-----------|--------------------------------------------------------------------------------|
| 1   | 1939      | Cracking Military Codes (BOMBE)                                                |
| 2   | 1940      | The First Ethical Pirate (Rene CARMILLE)                                       |
| 3   | 1982      | Siberian Gas Pipeline Attack                                                   |
| 4   | 1999      | NASA and the Department of Defense Cyber Attack.                               |
| 5   | 1999      | Melissa Virus                                                                  |
| 6   | 2003      | Titan Rain                                                                     |
| 7   | 2004      | Sven Jaschan vs Delta Airlines                                                 |
| 8   | 2005      | Alberto Gonzalez                                                               |
| 9   | 2006-2010 | Stuxnet Attack                                                                 |
| 10  | 2007      | Estonia Cyber Attacks                                                          |
| 11  | 2007      | Hacking of Pentagon E-mail Accounts                                            |
| 12  | 2008      | Cyber Attacks On Georgia During The Russian-Georgian War                       |
| 13  | 2008      | Cyber Attack On US Military Computers                                          |
| 14  | 2009      | Vulcanbot Attacks                                                              |
| 15  | 2010      | Myanmar (Bruma) Attacks                                                        |
| 16  | 2010      | Japan-South Korea Cyber Wars                                                   |
| 17  | 2010      | China's Alleged Cyberattacks On India.                                         |
| 18  | 2011      | Cyberattacks On Canadian Government And Commercial Business Sites              |
| 19  | 2011      | Wiper Attack                                                                   |
| 20  | 2011      | Theft of 24,000 files belonging to the US Department of Defense                |
| 21  | 2012      | Shamoon Virus                                                                  |
| 22  | 2013      | South Korean Cyber Attacks                                                     |
| 23  | 2013      | Singapore Cyber Attacks                                                        |
| 24  | 2013      | OpIsrael Attacks                                                               |
| 25  | 2013      | Adobe Systems Cyber Attack                                                     |
| 26  | 2014      | Operation Cleaver Attacks                                                      |
| 27  | 2014      | Yahoo Cyber Attack                                                             |
| 28  | 2015      | Attacks by Russian hackers on computer systems belonging to the US White House |
| 29  | 2017      | Ukraine Cyber Attacks                                                          |
| 30  | 2017      | WannaCry Ramsomware                                                            |
| 31  | 2018      | Marriott Hotels Cyber Attack                                                   |
| 32  | 2021      | RockYou2021                                                                    |

Ülkelerde yapılan çalışmalar ve stratejilerin kapsamlı bir şekilde incelenmesi, zaman geçtikçe siber güvenlik stratejilerinin kapsamının yalnızca vatandaşları veya hükümetleri siber saldırılara karşı güvence altına almaktan genel olarak tüm bilgi toplumunu güvence altına almaya doğru kaydığı gerçeğini de ortaya koymaktadır. Tablo 2.3'te dünya üzerinde gerçekleşen büyük siber olaylar sunulmuştur.

## 2.1.1. Yazılım Mühendisliği ve Türkiye'nin Siber Güvenlik Politikaları

### 2.1.1.1. Yetkili Kuruluşlar ve İlk Çalışmalar

Siber güvenlik alanında dünya çapında gerçekleştirilen çalışmalar ve oluşan farkındalık ile birlikte Türkiye'de de bu anlamda bir farkındalık oluşmuş, bu anlamda çalışmalar yapılmaya

başlanmıştır. Bu farkındalığı kişisel ya da ticari girişimlerle değerlendirmekten ziyade devlet eliyle kamusal anlamda değerlendirmenin daha doğru olacağı düşünülmektedir. Devlet eliyle gerçekleşen farkındalık sonucunda yapılan politikalar, çalışmalar ve hukuki düzenlemeler profesyonel adımlar olarak değerlendirilir.

Türkiye’de bu anlamda temel olarak atılmış ilk adım siber suç teriminin ilk kez ortaya atılmasıdır. Bu doğrultuda 3756 Sayılı olarak 1991 yılında yayımlanan “Türk Ceza Kanunu”nda meydana gelen değişikliklerde bilişim alanında gerçekleşen kötücül faaliyetler yasayla ceza olarak belirlenmiştir. Bilişim alanında hukuksuz olarak ele geçirilen bilgilerin kullanılmasını, işlenmesini, dağıtılmasını suç olarak tanımlayan değişiklik maddesiyle uzun bir süre Türkiye’de bu alanda kayda değer bir çalışma yapılamamıştır. Ancak ilerleyen süreçle birlikte bakıldığı zaman, kayda değer adımın Türkiye’de siber güvenlik politikalarının oluşmasında ilk adım, 1997 yılında Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu (TÜBİTAK) bünyesinde gerçekleşen “Siber Güvenlik Enstitüsü”nün kuruluşu olarak değerlendirilebilmektedir. Bu enstitünün kurulması ile yürütülen çalışmalar ile başta test laboratuvarı kurulmuş olup Microsoft ve Türkiye’de kullanılan benzer açık kaynak kodlu olarak sunulan işletim sistemleri güvenlik anlamında değerlendirilmiştir. Bu işletim sistemleri üzerinde entegre çalışan ağ cihazları, sunucular, Saldırı Tespit Sistemleri (STS), veri tabanları, uygulamalar da geniş bir perspektifle değerlendirilmiştir [44, 45].

Tablo 2.3’de Türkiye’de dijitalleşme ve siber güvenlik faaliyetleri alanında önemli sayılabilecek diğer adımlardan bazılarına yer verilmiştir.

**Tablo 2.4:** Türkiye’de dijitalleşme ve siber güvenlik faaliyetleri alanında önemli adımlar

| KURUM/KURULUŞ                         | ÖNEMLİ FAALİYETLER                                   |
|---------------------------------------|------------------------------------------------------|
| Dünya Bankası (1993):                 | Türkiye, Bilişim ve Ekonomik Modernizasyon Raporu    |
| Ulaştırma Bakanlığı-TÜBİTAK (1999):   | TUENA Türkiye Ulusal Enformasyon Altyapısı Ana Planı |
| Dış Ticaret Müsteşarlığı (1998-2002): | e-Ticaret Koordinasyon Kurulu                        |
| Başbakanlık (1998-2002):              | KamuNET                                              |
| Türkiye Bilişim Derneği (Mayıs 2002): | Türkiye Bilişim Şurası                               |
| Başbakanlık (2001-2002):              | e-Türkiye Girişimi                                   |
| TÜBİTAK (2002-2004):                  | Vizyon 2023                                          |

Test laboratuvarı çalışmalarının sonunda gerçekleşen bir diğer önemli adım Genelkurmay Başkanlığı tarafından verilen destek ile Ortak Kriter Test Merkezi (OKTEM) kurulması fikri bir proje olarak 2000 yılında gerçekleştirilmiş ve müteakiben 2001 yılında bu projenin bir ürünü olarak kurulmuştur. 2005 yılından bugüne kadar da sertifikasyon, lisanslama, akreditasyon çalışmaları, günümüze akıllı kart güvenliği gibi konularda çeşitli alanlarda faaliyetlerine devam etmiştir. Bu alandaki faaliyetler ile dünya üzerinde önemli bir test ve değerlendirme merkezi olarak kendini kanıtlamıştır [46, 47].

Türk Silahlı Kuvvetleri (TSK)'nin da bilgi güvenliği anlamındaki gereksinimlerini ve değerlendirmelerini gerçekleştirmek amacıyla kurulan “Ağ Güvenliği Grubu”, birçok çalışma ve proje gerçekleştirmiştir. Bu anlamda gerçekleşen çalışmalar, güvenli mimarilerin ve sistemlerin kurulum, test, risk değerlendirmesi vb. alanlarda yapılan projelerle bilişim altyapısında siber farkındalığın sağlanmasında otorite sağlayıcı bir çerçeve oluşturmuştur [47, 48].

Önceki yıllarda birçok farklı adla gerçekleştirilen çalışmalarda bütünlük olmadığı ve ülkenin öncelikli ihtiyaçları kapsamında yapılmadığı görülmektedir. Kurumların güvenliği temel alınarak yapılan çalışmalar bir türlü istikrar sağlayamamıştır. Ancak bilgi toplumu olmaya giden yolda bütüncül çalışmanın zorunluluğu ortaya çıkmış olup bu nedenle hükümet eliyle “Acil Eylem Planı” hazırlanmıştır; bu planda “e-Dönüşüm Türkiye Projesi”ne de dikkat çekilmiştir. Türkiye'nin elektronik çalışmaları kapsamında önemli bir adım olan proje üzerinde yetkili kuruluş olarak “Devlet Planlama Teşkilatı (DPT) Müsteşarlığı” belirlenmiştir. Bu gelişmelerin ardından 27 Şubat 2003 tarihinde yayımlanan “Başbakanlık Genelgesi”nde söz konusu projenin hedefleri, esasları ve yapısı belirlenmiştir. DPT üzerine aldığı bu görev ile birlikte çalışmalarına başlamış ve yine aynı yılın mart ayında “Bilgi Toplumu Dairesi (BTD)”ni bünyesinde kurmuştur.

Ağ Güvenliği Grubu, gerçekleştirdiği bu çalışmalar ile birlikte toplumsal farkındalık oluşturmak ve ülke çapında bir bilinç oluşturmak amacıyla özel sektöre de ulaşmak gerektiği için yine önemli adımlar atmıştır. Özellikle kritik özel sektör kurumları ile değerlendirmeler yaparak projeler yapmıştır. Başta bu anlamda test faaliyetleri ile başlayan adımlar sonrasında kuruluşlara dair risk değerlendirmeleri, sistem kurulumları ve danışmanlıklar sağlayarak farkındalığın kapsamını artırmıştır.

BTD'nin 2003 yılında kurulmasının ardından başlatmış olduğu “Bilgi Toplumu Stratejisi” adlı proje çalışmasını Türkiye’de bilgi ve iletişim sistemleri alında çok önemli bir adım olarak değerlendirilmektedir. Bilgi toplumu olarak teknolojik gereksinimlere ayak

uydurma amacıyla gerçekleştirilen çalışma, önemli bir ölçüde yol kat etmiştir. “Bilgi Toplumu Stratejisi”nin maddeleri arasında yer alan ve faaliyetlerinin “Ağ Güvenliği Grubu” tarafından yürütülen güvenlik programı, öncelikle kamusal alanda güvenlik alanında ihtiyaçları karşılamayı hedeflemiştir. Bu program sayesinde birçok kamu kurumunda örnek çalışmalar yapılmış, kamudaki güvenlik problemlerini azaltmak ve bu alanda farkındalık oluşturmak adına önemli adımlar atılmış, çalışanlara ve bilişim personeline eğitimler verilmiştir. Daha sonrasında “Sistemlerin Güvenlik Programı” adlı projenin devamı olarak değerlendirilen “Kamu Bilgi Güvenliği” adlı projeyle de kamu kurumlarında görev yapan personele çeşitli eğitimler verilmiştir. Bu eğitimlerle büyük oranda farkındalık oluşturulmuş ve bilgi güvenliği alanında yaşanan olaylara uygun bir aksiyon alınmasını sağlayan politika izlenmesi sağlanmıştır. Bu hedef doğrultusunda 2008 yılında kurulan “Bilgisayar Olaylarına Müdahale Ekibi” ile bilgi güvenliği konularında ulusal tatbikat, değerlendirme, eğitim ve koordinasyon faaliyetleri sağlayarak sorunlara anında tepki verecek kapasiteye sahip olmak amaçlanmıştır [42, 43].

Bu değerlendirmeler ile birlikte siber güvenlik anlamında önemli bir adım atılmış olarak kabul edilmektedir. Yapılan çalışmalarda bu ortak kriterlerin belgelendirmesi hususunda 2010 yılında “Türk Standartlar Enstitüsü (TSE)” ve TÜBİTAK’ın ortak çalışmalarının bir ürünü olarak sertifika üreticisi olan ülkeler arasında oluşan uluslararası sıralamada ülkemiz 14. olarak yerini almıştır. Türkiye'nin önemli diğer siber güvenlik strateji belgeleri ve planları Tablo 2.4’te sunulmuştur.

**Tablo 2.5:** Türkiye’nin dijitalleşme ve siber güvenlik faaliyetleri alanında önemli adımları

| KONU                                                                                                                | SORUMLU MAKAM                          | TARİH     |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----------|
| Bilgi Toplumu Stratejisi ve Eylem Planı                                                                             | Kalkınma Bakanlığı                     | 2006–2010 |
| Ulusal Sanal Çevre Güvenlik Politikası                                                                              | Sanayi ve Ticaret Bakanlığı            | 2009      |
| Türkiye Siber Güvenlik Teşkilatı ve Yol Haritası                                                                    | Sanayi ve Teknoloji Bakanlığı          | 2012      |
| Siber Güvenlik Kurulu Oluşumu                                                                                       | Ulaştırma Bakanlığı ve Altyapı         | 2012      |
| Ulusal Siber Güvenlik Stratejisi ve Eylem Planı                                                                     | Ulaştırma Bakanlığı ve Altyapı         | 2013-2014 |
| Bilgi Toplumu Stratejisi ve Eylem Planı                                                                             | Kalkınma Bakanlığı                     | 2015–2018 |
| Kişisel Verilerin Korunması Kanunu                                                                                  | Adalet Bakanlığı                       | 2016      |
| Ulusal e-Devlet Stratejisi ve Eylem Planı                                                                           | Ulaştırma ve Altyapı Bakanlığı         | 2016–2019 |
| Ulusal Siber Güvenlik Stratejisi ve Eylem Planı                                                                     | Ulaştırma ve Altyapı Bakanlığı         | 2016–2019 |
| Bilgi Teknolojileri ve İletişim Kurumuna siber caydırıcılık sağlamak için görev vermek veya her türlü tedbiri almak | Ulaştırma ve Altyapı Bakanlığı         | 2016      |
| Türkiye Yazılım Sektörü Stratejisi ve Eylem Planı                                                                   | Kalkınma Bakanlığı                     | 2017–2019 |
| Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi                                                   | Cumhurbaşkanlığı Dijital Dönüşüm Ofisi | 2019      |
| Bilgi ve İletişim Güvenliği Rehberi                                                                                 | Cumhurbaşkanlığı Dijital Dönüşüm Ofisi | 2020      |
| Bilgi ve İletişim Güvenliği Denetim Rehberi                                                                         | Cumhurbaşkanlığı Dijital Dönüşüm Ofisi | 2021      |

Zaman geçtikçe kalıplarını genişleten ve ülkemizin önemli güvenlik merkezine dönüşen Ağ Güvenliği Grubu’nun ismi de ilk olarak “Bilişim Sistemleri Güvenliği Bölümü” olmuştur. Siber Güvenlik Enstitüsü teşkilatındaki varlığını ise 2012 Temmuz ayından itibaren sürdürmektedir. Söz konusu enstitü hâlihazırda TSK, özel şirketler ve devlet kurumlarıyla çalışmalar yapmakta ve projeler gerçekleştirmektedir [44].

“e-Dönüşüm Türkiye Projesi”nin faaliyetlerinin yürütülmesinde dönemsel olarak değişen, e-Türkiye Girişimi neticesinde meydana gelen ve bir takım düzenlemeler yapılan çalışma grupları ve bağlı oldukları kurum bilgileri Tablo 2.5’te verilmiştir.

**Tablo 2.6:** E-Türkiye Girişimi neticesinde çalışmalar ve sorumlu kurumlar [49]

| <b>ÇALIŞMA GRUBU</b>                             | <b>YETKİLİ KURUM</b>                   |
|--------------------------------------------------|----------------------------------------|
| Eğitim ve İnsan Kaynakları Çalışma Grubu:        | Milli Eğitim Bakanlığı                 |
| Teknik Altyapı ve Bilgi Güvenliği Çalışma Grubu: | Ulaştırma Bakanlığı                    |
| Hukuki Altyapı Çalışma Grubu:                    | Adalet Bakanlığı                       |
| e-Devlet Çalışma Grubu:                          | Devlet Planlama Teşkilatı              |
| e-Ticaret Çalışma Grubu:                         | Dış Ticaret Müsteşarlığı               |
| Standartlar Çalışma Grubu:                       | Türk Standartları Enstitüsü Başkanlığı |
| e-Sağlık Çalışma Grubu:                          | Sağlık Bakanlığı                       |
| İzleme Çalışma Grubu:                            | Türkiye Bilişim Derneği                |

Özellikle siber güvenliğin ve savunmanın günümüzde çok önemli bir duruma gelen kritik altyapıların gitgide daha akıllı olması bu tür altyapıların üzerindeki risk ihtimalini de yükseltmiştir.

Siber Güvenlik Enstitüsü tarafından risk ihtimali yüksek ve misyon olarak ülke için büyük önem arz eden kritik altyapı sistemlerini (su, haberleşme, finans, enerji vb.) korumaya yönelik Kalkınma Bakanlığı tarafından verilen destekle çalışma başlatılmıştır. Bu sistemlerin olası tehditleri için raporlar hazırlanmış, bazı yapılarda Denetim Kontrolü ve Veri Toplama (SCADA) sistemlerine yönelik güvenliğe dair testlerini gerçekleştirmişlerdir. Bu alanda yapılan ciddi çalışmalar ve oluşan birikimle birlikte, İş Sürekliliği ve Bilgi Güvenliği Yönetim Sistemi vb. sahalarda başarılı sonuçlar elde etmişler; Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization-NATO) kapsamında ortak çalışmalar yapılmıştır [50].

Türkiye’de kritik altyapıların korunmasında ve siber uzayda oluşan krizleri yönetme sorumluluğu “Afet ve Acil Durum Yönetimi Başkanlığı (AFAD)”nın Teşkilat ve Görevleri Hakkında çıkan 5902 sayılı Kanun ile AFAD’a verilmiştir. AFAD bu yükümlülüğüyle birlikte afet tanımını, doğal afet ve teknolojik olarak ikiye ayırmıştır. Kritik altyapıların korunması ile siber güvenlik faaliyetleri bu kategorilerden teknolojik afetlerde yerini almıştır.

Kritik Altyapı Koruma Planı çerçevesinde AFAD, bakanlıklar, Hacettepe Üniversitesi gibi kurumlar seçilerek bu plana dâhil edilmiştir. AFAD, kritik alt yapıların korunmasına yönelik temel adımlar için, bu sektörde Avrupa Birliği (AB)’nin talimatlarını da dikkate almak ve paydaşlarla etkin bir çalışma, koordinasyon ve işbirliği sağlamak için 2014 yılının eylül ayında “2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi”ni yayınlamıştır [27].

11 Haziran 2012 tarihinde Bakanlar Kurulu tarafından alınan “Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar”ın (2012/3842

sayısıyla), Resmi Gazete’de yayımlanmasıyla yürürlüğe konulmuştur. Söz konusu karar ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı’na siber faaliyetler anlamında yetki ve görevler verilerek “Siber Güvenlik Kurulu” oluşturulmuştur. Tablo 2.7’de Siber Güvenlik Kurulu’nun teşkilatı ve görevleri sunulmuştur.

**Tablo 2.7: Siber Güvenlik Kurulu’nun teşkilatı ve görevleri**

| <b>SİBER GÜVENLİK KURULUNUN GÖREVLERİ</b>                                                                                                                                                                       |                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak                                                          | Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak                                                                                                                                                                                 |
| Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek                                                                                              | Kanunlarla verilen diğer görevleri yapmak.                                                                                                                                                                                                            |
| <b>SİBER GÜVENLİK KURULUNUN TEŞKİLATI</b>                                                                                                                                                                       |                                                                                                                                                                                                                                                       |
| Dışişleri Bakanlığı Müsteşarı,<br>Milli Savunma Bakanlığı Müsteşarı,                                                                                                                                            | İçişleri Bakanlığı Müsteşarı,<br>Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,                                                                                                                                                             |
| Kamu Düzeni ve Güvenliği Müsteşarı,<br>Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,<br>Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı,<br>Telekomünikasyon İletişim Başkanı | Milli İstihbarat Teşkilatı Müsteşarı,<br>Bilgi Teknolojileri ve İletişim Kurumu Başkanı,<br>Mali Suçları Araştırma Kurulu Başkanı,<br>Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticileri |

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı’nın öncülüğünde “2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı” ile benzerlik göstererek bu plan doğrultusunda ihtiyaçlara daha sağlam çözümler sunacak geçmiş tecrübelerle uluslararası çalışmaları koordineli bir şekilde yürütmek amacıyla “2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı” belgesi yayımlanmıştır. Girişimciliğe, yenilikçiliğe ve yüksek katma değerli teknoloji üretimine dayalı ekonomik yapısıyla, Avrasya’nın mal ve hizmet üretim üssü haline gelen ve dünyanın en gelişmiş on ülkesi içinde yer alan bir Türkiye’nin oluşumunda öncü olmak” vizyonu ışığında, dünya üzerinde gelişmiş ülkeler sıralamasında sıralamaya girmek, girişimci yaklaşımıyla yeni ve katma değer sağlayacak bir teknoloji odaklı ekonomik yapı oluşturmak bilinciyle öncü olmak amacıyla düzenlenmiştir. Bu plan ticaret, sanayi ve üretim alanında köklü değişiklikler sağlamak amacıyla ulusal politikaların göz önünde bulundurulması amacıyla hazırlanmıştır.

Yapılan hazırlıklar temelinde çalıştaylar gerçekleştirilmiş kurum ve kuruluşlarla yapılan toplantılarda ortaya çıkan görüşler neticesinde hedefler 4 temel başlık altında belirlenmiştir. Strateji belgesinin hazırlanmasına yönelik olarak düzenlenen çalıştayın sonucu olarak, alâkalı

kurumların, kuruluşların değerlendirmeleri ve önemli toplantılar sonucunda temelde 4 hedef başlığı meydana gelmiştir. Bu hedefleri gerçekleştirmekten sorumlu olan kuruluşlar, ilgili kuruluşlar ve eylemlerin gerçekleştirilmesi için gerekli süreler, performans göstergeleri ile her bir eyleme ilişkin açıklamaları içeren eylem planı hazırlanmıştır. Belirlenen hedefler Tablo (2.7, 2.8, 2.9 ve 2.10)'da belirtilmiş; ayrıca stratejiye yönelik eylem planları açıklanmıştır.

**Tablo 2.8:** 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 1 [52]

| <b>HEDEF 1: ULUSAL BİLİNCİ ARTIRMAK VE ALTYAPIYI GÜÇLENDİRMEK</b>                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EYLEM 1.1: TÜBİTAK-BİLGEM’de yer alan Siber Güvenlik Enstitüsü; “Bilgi Güvenliği ve Siber Güvenlik Enstitüsü” adı altında yeniden yapılandırılacaktır.                                 |
| EYLEM 1.2: Kamu kurum ve kuruluşlarının yazılım ürünü ihtiyaçları belirlenecek ve bu ihtiyaçların kaliteli ve güvenli karşılanmasına yönelik sınıflama çalışmaları yapılacaktır.       |
| EYLEM 1.3: “Bilişim Firmaları Belgelendirme/Yetkilendirme Sistemi” kurulacaktır.                                                                                                       |
| EYLEM 1.4: Bilişim Firmalarına "Yetki Belgesi" verilmesine yönelik mevzuat düzenlemesi yapılacaktır.                                                                                   |
| EYLEM 1.5: Yazılımın tüm sektörler için öneminin kamuoyunda bilinirliğinin artırılmasına yönelik kamu spotu hazırlanacaktır.                                                           |
| EYLEM 1.6: Ulusal düzeyde yıllık yazılım geliştirme yarışmaları düzenlenecektir.                                                                                                       |
| EYLEM 1.7: Yazılım sektörüne ilişkin bir taksonomi çalışması gerçekleştirilecek ve terimler kılavuzu oluşturulacaktır.                                                                 |
| EYLEM 1.8: Yazılım sektöründe Fikri ve Sınai Mülkiyet Hakları konusunda yaşanan sorunların tespit edilmesine ve bu alanda farkındalığın artırılmasına yönelik çalışmalar yapılacaktır. |

**Tablo 2.9:** 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 2 [52]

| <b>HEDEF 2: HUKUKİ VE İDARİ DÜZENLEMELERİ YAPMAK</b>                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EYLEM 2.1: Yazılım sektörü ürünlerine ve güvenlik açıklarına yönelik kriter, standart ve belgelendirme sayısının artırılması sağlanacaktır.                         |
| EYLEM 2.2: Yerli yazılım firmalarına kamu alımlarında fiyat avantajı sağlayacak şekilde Kamu İhale Kanunu’nda düzenleme yapılacaktır.                               |
| EYLEM 2.3: Başta yazılım olmak üzere bilişim ürünlerinin kamu tedarikinde izlenecek süreçle yönelik düzenlemeler yapılacaktır.                                      |
| EYLEM 2.4: Akredite yazılım test merkezlerinin kurulması sürecine yönelik destek mekanizması geliştirilecektir.                                                     |
| EYLEM 2.5: Yerli yazılım ürünlerinin akredite test ve belgelendirme merkezlerindeki test ve sertifikasyon süreçlerine yönelik destek mekanizması geliştirilecektir. |
| EYLEM 2.6: Kamu kurumlarının yazılım alımları için genel teknik şartname hazırlanacaktır.                                                                           |
| EYLEM 2.7: Bilişim suçları alanındaki hukuki eksikliklerin tespitine ve bu eksikliklerin giderilmesine yönelik çalışma yapılacaktır.                                |
| EYLEM 2.8: Sayısal kod emanetçiliği sistemi hayata geçirilecektir.                                                                                                  |

**Tablo 2.10:** 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 3 [52]

| <b>HEDEF 3: NİTELİKLİ İNSAN KAYNAĞI GELİŞTİRMEK</b>                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EYLEM 3.1: Sektörün yıllık işgücü ihtiyacı belirlenecektir.                                                                                                                                              |
| EYLEM 3.2: Bilgisayar bilimleri ve programlama kültürünün erken yaşlarda edinilmesine yönelik müfredat çalışması yapılacaktır.                                                                           |
| EYLEM 3.3: Sektörün nitelikli eleman ihtiyacını karşılamak için meslek liselerinin ilgili bölümlerinin müfredatı güncellenecektir.                                                                       |
| EYLEM 3.4: Üniversitelerin bilgisayar ve yazılım mühendisliği bölümlerinde, sektörün ihtiyacı doğrultusunda müfredat güncelleme çalışmaları yapacak “Danışma ve Yönlendirme Kurulları” oluşturulacaktır. |
| EYLEM 3.5: Yazılım alanında ulusal ve uluslararası yarışmalarda dereceye giren öğrencilere ödül/destek verilmesine yönelik düzenleme yapılacaktır.                                                       |
| EYLEM 3.6: Yurtdışında konuyla ilgili öncelikli alanlarda lisansüstü eğitim görenlere verilen burs ve desteklerden yararlanıcı sayısı artırılacaktır.                                                    |
| EYLEM 3.7: Yazılım sektöründe uygulama deneyimine sahip yetkin kişilerin üniversitelerde eğitim-öğretim süreçlerine katkı vermeleri sağlanacaktır.                                                       |
| EYLEM 3.8: Sektörün ihtiyacı olan nitelikli personel yetiştirilmesinde uzaktan eğitim yönteminin kullanımı yaygınlaştırılacaktır.                                                                        |
| EYLEM 3.9: İstihdama katılmayan genç işgücüne bilgisayar ve yazılım yetkinlikleri kazandıracak eğitimler verilerek istihdam artırılacaktır.                                                              |

**Tablo 2.11:** 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı hedef 4 [52]

| <b>HEDEF 4: ULUSLARARASI REKABET GÜCÜNÜ ARTIRMAK</b>                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EYLEM 4.1: Türkiye’nin uluslararası yazılım sektöründe fark yaratabileceği öncelikli alanlar belirlenerek, bu alanlara yönelecek girişimcilere özel tematik destek programı hazırlanacaktır.      |
| EYLEM 4.2: Başta Teknoloji Geliştirme Bölgeleri olmak üzere, sektörün güçlü olduğu Bölgelerde yazılım firmalarına ve girişimcilerine yönelik “Yazılım Hızlandırıcı Programları” oluşturulacaktır. |
| EYLEM 4.3: Yazılım sektörü kapsamında yurtdışı potansiyel pazarların analizine yönelik yıllık düzenli raporlama çalışması yapılacak ve firmalara duyurulacaktır.                                  |

Cumhurbaşkanlığı Teşkilatı kararnamesi ile kurulan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO)’ne siber ve bilgi güvenliğini farkındalığını artırmak ve güvenliğini sağlamak için politikalar ve projeler geliştirme sorumluluğu verilmiştir. Bu kapsamda yapılan çalışmalar neticesinde Cumhurbaşkanlığı tarafından 6/7/2019 tarihli “Bilgi ve İletişim Güvenliği Tedbirleri” genelgesi yayımlanmış ve çalışma grubu kurulmuştur. Bu genelge kapsamında çalışmaları geliştirmesi amacıyla oluşturulan “Bilgi ve İletişim Güvenliği Rehberi”, tüm bu görev ve sorumluluklarla kurumların yapması gerekenleri içermektedir. Rehber tam anlamıyla uyarken yerine getirmesi gereken bir diğer adım da denetim sürecini tamamlamak için çıkarılan 10 Kasım 2021 tarihinde “Bilgi ve İletişim Güvenliği Denetim Rehberi”dir. Rehberde yer alan maddeler ve politikalar kapsamında kurumlar belirli çalışmaları yerine getirmekle sorumlu olmuştur. Yapılması gereken bu çalışmalar; plan, uygulama, kontrol, yönetme, önlem gibi süreçleri bir çerçevede yürütülmelidir. Bu anlamda denetim faaliyetlerinin

yıl içerisinde en az bir defa gerçekleştirilmesi, kurumların da gereken planları yapması ve işletmesi gerekmektedir. Denetim faaliyetlerinin de verimli bir şekilde gerçekleştirilmesi amacıyla düzgün bir yöntemle de gerçekleştirilmesi, faaliyetlerin etkinliği açısından önemlidir. Gerçekleştirilecek denetim çalışmalarının bağımsız olması, raporlanması ve kurumlara/denetçilere bakış açısı ve rapor oluşturulması açısından bu rehberin hazırlandığı görülmektedir [45-52].

#### **2.1.1.2. Eğitim Faaliyetleri ve Yazılım Mühendisliği Değerlendirmesi**

Yazılım mühendisliği, sistematik bir uygulamanın tüm yazılım geliştirme sürecine yönelik bir mühendislik yaklaşımıdır. Yazılım mühendisi, bilgisayar yazılımını tasarlamak, geliştirmek, sürdürmek, test etmek ve değerlendirmek için yazılım mühendisliği ilkelerini uygulayan kişidir. Programcı terimi yazılımcı olarak nitelendirilse de mühendislik eğitimi veya becerilerinin çağrışımlarından da yoksun olabilmektedir. Yazılım mühendisliği eğitimini alan kişi, mühendislik teknikleri, yazılım yaşam döngüsü sürecinin tanımlanması, uygulanması, değerlendirilmesi, ölçülmesi, yönetimi, değiştirilmesi ve iyileştirilmesini içeren yazılım geliştirme sürecinin tümüne hakimdir. Ayrıca yazılım geliştirme sürecindeki değişiklikleri sistematik olarak kontrol etmek ve sistem yaşam döngüsü boyunca konfigürasyon ve kodun bütünlüğünü ve izlenebilirliğini korumakla yükümlü kişidir.

Yazılım mühendisliği, 1960'lardan başlayarak ayrı bir mühendislik türü olarak görülmeye başlamıştır. Ancak, yazılım mühendisliğinin gelişimi bir mücadele ile geçmiştir. Yazılım mühendisliği için bir milat olarak 1968'de NATO'nun, yazılımla ilgili konuları ele aldığı ilk yazılım mühendisliği konferansı sayılabilmektedir. Yazılım mühendisliği, genellikle, bir projenin ilk adımı ile başlamakta olup, kullanıcının projeyi teslim almasını, bakım-onarımı da kapsayan bir süreç olarak ele alınmaktadır.

Yazılım geliştirme ekibi, kullanıcı gereksinimleri, sistem gereksinimleri ve işlevsel gereksinimleri birbirinden ayırmaktadır. Gereksinim, bir kullanıcı ile görüşme yapılarak, bir veri tabanına atıfta bulunularak, mevcut sistem üzerinde çalışılarak toplanmaktadır. Gereksinim toplandıktan sonra ekip, yazılımın kullanıcının tüm gereksinimlerini karşılayacak şekilde yapıp yapılamayacağını analiz etmektedir. Geliştirici daha sonra proje planının bir yol haritasına karar vermektedir. Sistem analizi ayrıca yazılım ürünü sınırlamalarının anlaşılmasını da içermektedir. İhtiyaç ve analizlere göre yazılım tasarımı yapılmakta; yazılım tasarımının uygulanması, uygun bir programlama dilinde program kodunun yazılmasıyla başlamaktadır. Yazılım testleri, geliştiriciler tarafından kodlanırken yapılır ve test uzmanları tarafından modül

testi, program testi, ürün testi, kurum içi test ve kullanıcının katılımı ve geri bildiriminde ürünü test etme gibi çeşitli kod seviyelerinde kapsamlı testler yapılmaktadır [53]. Tüm bu süreçlerin yönetiminde de yazılım mühendisi eğitime sahip kişi görev almaktadır. Tablo 2.11’de dünyada yazılım mühendisliği eğitiminde en iyi üniversiteler, Tablo 2.12’de ise Türkiye’de yazılım mühendisliği eğitimi veren üniversiteler sunulmuştur.

**Tablo 2.12:** Dünyada yazılım mühendisliği eğitiminde en iyi üniversiteler

| ÜNİVERSİTE ADI                                         | DERECE                           |
|--------------------------------------------------------|----------------------------------|
| Oxford Üniversitesi                                    | Lisans, Yüksek Lisans ve Doktora |
| Stanford Üniversitesi                                  | Lisans, Yüksek Lisans ve Doktora |
| Massachusetts Teknoloji Enstitüsü (MIT)                | Lisans, Yüksek Lisans ve Doktora |
| Cambridge Üniversitesi                                 | Lisans, Yüksek Lisans ve Doktora |
| ETH Zürih (Eidgenössische Technische Hochschule Zürih) | Lisans, Yüksek Lisans ve Doktora |
| Carnegie Mellon Üniversitesi                           | Lisans, Yüksek Lisans ve Doktora |
| Harvard Üniversitesi                                   | Lisans, Yüksek Lisans ve Doktora |

**Tablo 2.13:** Türkiye’de yazılım mühendisliği eğitimi veren üniversiteler [54]

| TÜRKİYE’DE YAZILIM MÜHENDİSLİĞİ EĞİTİMİ                            |                                                             |                                                    |                                                     |
|--------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------|
| Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi (İngilizce) | Ankara Bilim Üniversitesi (İngilizce) (Ücretli)             | İstanbul Okan Üniversitesi (İngilizce) (Burslu)    | Muş Alparslan Üniversitesi (4 Yıllık)               |
| Ankara Yıldırım Beyazıt Üniversitesi (İngilizce)                   | Antalya Akev Üniversitesi (Burslu)                          | İstanbul Sabahattin Zaim Üniversitesi (Burslu)     | Orta Doğu Teknik Üniversitesi (İngilizce) (Ücretli) |
| Atatürk Üniversitesi                                               | Atılım Üniversitesi (İngilizce) (Burslu)                    | İstanbul Sağlık ve Teknoloji Üniversitesi (Burslu) | Girne Üniversitesi (Burslu)                         |
| Bandırma Onyedli Eylül Üniversitesi                                | Bahçeşehir Üniversitesi (İngilizce) (Ücretli)               | İstinye Üniversitesi (Burslu)                      | Doğu Akdeniz Üniversitesi (İngilizce) (Ücretli)     |
| Burdur Mehmet Akif Ersoy Üniversitesi                              | Beykent Üniversitesi (Burslu)                               | Ankara Bilim Üniversitesi (İngilizce) (Ücretli)    | Sakarya Üniversitesi (İngilizce) (4 Yıllık)         |
| Fırat Üniversitesi                                                 | Beykoz Üniversitesi (Burslu)                                | Antalya Akev Üniversitesi (Burslu)                 | Toros Üniversitesi (İngilizce) (Burslu)             |
| Muğla Sıtkı Koçman Üniversitesi (İngilizce)                        | Çankaya Üniversitesi (İngilizce) (Burslu)                   | Atılım Üniversitesi (İngilizce) (Burslu)           | Türk Hava Kurumu Üniversitesi (İngilizce) (Ücretli) |
| Gümüşhane Üniversitesi                                             | Doğu Üniversitesi (Burslu)                                  | Bahçeşehir Üniversitesi (İngilizce) (Ücretli)      | Üsküdar Üniversitesi (İngilizce) (Burslu)           |
| İnönü Üniversitesi                                                 | Fatih Sultan Mehmet Vakıf Üniversitesi (İngilizce) (Burslu) | Rauf Denktaş Üniversitesi (İngilizce) (Burslu)     | Yaşar Üniversitesi (İngilizce) (Ücretli)            |

|                                     |                                                        |                                                              |                                                          |
|-------------------------------------|--------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------------|
| Karadeniz Teknik<br>Üniversitesi    | Haliç Üniversitesi<br>(İngilizce) (Burslu)             | Uluslararası Final<br>Üniversitesi (İngilizce)<br>(Burslu)   | Samsun Üniversitesi                                      |
| Kırklareli Üniversitesi             | Hasan Kalyoncu<br>Üniversitesi (İngilizce)<br>(Burslu) | Uluslararası Kıbrıs<br>Üniversitesi (İngilizce)<br>(Ücretli) | Altınbaş Üniversitesi (İngilizce)<br>(Burslu) (4 Yıllık) |
| Kocaeli Üniversitesi                | Işık Üniversitesi<br>(İngilizce) (Ücretli)             | Yakın Doğu Üniversitesi<br>(Burslu)                          | Maltepe Üniversitesi (İngilizce)<br>(Ücretli)            |
| Konya Teknik<br>Üniversitesi        | İstanbul Atlas<br>Üniversitesi (İngilizce)<br>(Burslu) | Lefke Avrupa Üniversitesi<br>(İngilizce) (Burslu)            | Nişantaşı Üniversitesi (İngilizce)<br>(Ücretli)          |
| Malatya Turgut Özal<br>Üniversitesi | İstanbul Aydın<br>Üniversitesi (İngilizce)<br>(Burslu) | İstanbul Gelişim<br>Üniversitesi (Ücretli)                   | Ostim Teknik Üniversitesi (Burslu)<br>(4 Yıllık)         |
| Manisa Celâl Bayar<br>Üniversitesi  | İstanbul Ayvansaray<br>Üniversitesi (Burslu)           | İzmir Ekonomi Üniversitesi<br>(İngilizce) (Burslu)           | Ted Üniversitesi (İngilizce) (Ücretli)                   |

Yazılım mühendisliği; çözülecek probleme genel mühendislik ilkelerinin kullanılarak sonuç elde edilmesi; ekonomik, sistematik, güvenli, organize ve verimli çalışan yazılım elde etmek için uygulanmasıdır. Yazılım mühendisleri geliştirecekleri yazılımlarda bir dizi mühendislik tekniklerini kullanarak kalite artırmaya çalışmaktadır. Yazılım mühendisliği, bilgisayar mühendisliği gibi bilgisayar bilimlerinin bir alt birimi olsa da uygulamada tamamen aynı değildir.

Yazılım eğitimi, bilgisayar mühendisliği bölümlerinde yazılım derslerinin verilmesi, yazılıma dair kurslar verilmesi şeklinde de gerçekleşmektedir. Ancak mühendislik belirli bir konuya bütüncül yaklaşımdır, bu anlamda ülkemizde yazılım öğrenmede diğer yöntem ise yazılım mühendisliği bölümüdür. İlk kez 2005 yılında Atılım Üniversitesi'nde kurulmuş olup bir devlet üniversitesinde kurulması ise ilk kez 2009 yılında Fırat Üniversitesi'nde açılmasıyla olmuştur. Hâlihazırda Türkiye'de yazılım mühendisliği alanında eğitim veren üniversitelerin sayısı artmıştır.

Mevcut durumda birçok üniversitede kurulmuş olması sebebiyle bilim dalının ülkemizde halâ daha yeni olarak sayılması sebebiyle diğer mühendislik dallarına göre daha güncel olarak değerlendirilebilir. Üniversitelere göre farklı müfredatların verildiği görülse de temelde bilimsel, teorik ve pratik temelde bir eğitim planlamaları bulunmaktadır. Bölümün ilk yılında daha çok diğer mühendislik programlarının ve özellikle de bilgisayar mühendisliğinin ilk ve ikinci yılındaki derslerle benzerlikler olduğu görülmektedir. Üniversitelerde temelde

Matematik, İstatistik, Fizik, Kimya vb. dersler ortak olarak verilmektedir. Yazılım mühendisliğinde dersler çok daha uygulamaya yöneliktir ve sistemden ziyade yazılım konularına ağırlık verilmektedir. Yazılım mühendisliğini ayıran bir diğer konu da derslerin uygulama temelli olarak yazılım analizi, tasarımı, proje yönetimi, testi, işyeri eğitimi gibi avantajlara sahip olmasıdır [9, 53-55].

### **2.1.1.3. Hukuki Tedbirler**

#### **1991 Yılında 765 Sayılı Türk Ceza Kanunu’na Bilişim Suçları Maddesinin Eklenmesi**

Türkiye’nin siber güvenlik alanında hukuksal anlamda yapmış olduğu ilk girişim 6 Haziran 1991 yılında 765 Sayılı Türk Ceza Kanunu’na “Bilişim Suçları” teriminin dâhil edilmesi ile olmuştur. Bu terimin eklenmesi ile dijital dünyada gerçekleşecek ve kamu düzeninin, kişisel hak ve hürriyetlerinin ihlaline yönelik yapılacak her türlü aykırılığa karşı önlem alınması sağlanmıştır. Bu madde ile Türkiye’de siber farkındalığın erken tarilerde olduğu değerlendirilmektedir.

Henüz anayasada haberleşme hürriyeti kavramının yer almadığı bu tarihte eklenen “Bilişim Suçları” başlığı altında bu suçların kapsamı belirlenmiş, korunacak hak ve hürriyetlerin neler olduğuna yer verilmiştir. Kişilerin özel hayatının gizliliği temelinde ele alınan maddeler, mülkiyet hakkı, haberleşme hürriyeti, ekonomik menfaatler, sırrın dokunulmazlığı gibi konuların teminatı ile halkın bilişim sistemlerine ve dijital dünyada yapacağı ekonomik işlemlerde güvenini kazanmaya yönelik olarak belirlenmiştir. Düzenlemenin yapıldığı tarihte anayasada özel hayat, hak ve hürriyetler gibi terimlerin bulunmasına rağmen kanun koyucular tarafından ilerleyen yıllarda doğrudan kişisel verilerin korunması kapsamında da fıkralar eklenmiştir [56].

#### **Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı**

Türkiye’de siber farkındalığın gelişmesine paralel olarak 1999 yılında Milli Savunma Bakanlığı’nın koordinatörlüğünü yürüttüğü “Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun” ismiyle bir çalışma gerçekleştirilmiştir. Çalışılan kanunla Başbakanlık’a bağlı olarak ulusal bilgi güvenliği birliği sağlanması amaçlanmıştır. Bu kapsamda oluşturulacak üst kurul ve tüzel kişilikte “Ulusal Bilgi Güvenliği Kurumu” adında bir başkanlık kurulması hedeflenmiştir. Üyeleri ve çalışma prensiplerinin belirlenmesi teşkilatın oluşturulmasına rağmen yürürlüğe girmesi konusunda anlaşma sağlanamadığı için tasarı aşamasında kalmıştır [56, 57].

### **5070 Sayılı Elektronik İmza Kanunu**

Dijital dünyanın oluşması ile hemen her alanın buraya taşınması sonucunda resmi belge ve düzenlemelerin gerekliliğinden ötürü 15 Ocak 2004 tarihinde, 5070 sayılı Elektronik İmza Kanunu Resmi Gazete’de yayımlanmış ve yürürlüğe girmiştir. Kanun ile dijital platformlarda hazırlanan belgelerde kullanılacak elektronik imzanın hukukî kapsamı, teknik prosedürleri ve kullanım esaslarını yayımlanmıştır. Elektronik imza aşamasında yer alan tüm tanım ve işleyişi aktaran Kanun’da ayrıca imzalamada oluşan verilerin yetkisiz kullanımına, denetim mekanizmasına ve elektronik sertifikalarda oluşacak sahtekârlıklara yönelik cezalara da yer verilmiştir. Kanun kapsamında yetkili olarak da 27 Ocak 2000 tarihinde kurulan "Telekomünikasyon Kurumu" belirlenmiştir [58].

### **5237 Sayılı Yeni Türk Ceza Kanunu**

Kişisel hak ve özgürlükleri korumanın yanında, kamuda düzen ve güvenliği sağlamak amacıyla suçun gerçekleştirilmesini önlemek amacıyla 26 Eylül 2004 tarihinde “Yeni Türk Ceza Kanunu” Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Suçun önlenmesi amacıyla detaylı bir kapsamda yayımlanan 97 sayfalık Kanun’da, ceza doğurucu suçun tanımı, yaptırımlar, tedbirler, özel hükümler, uluslararası suçlar, uygulama alanları, temel esaslar düzenlenmiştir. Temel hak ve hürriyetlerin korunmasını amaçlayan ve güvenli bir toplum oluşturmayı hedefleyen “Ceza Kanunu 244. Maddesi”nde bilişim alanındaki suçlara da yer verilmiş, siber alanda kişilerin sahip oldukları hak ve özgürlükleri de tanımlamıştır. Kanun’da bilişim alanında yaşanacak yetkisiz giriş, sistemin bütünlüğüne verilen zarar, verileri yok etme/değiştirme, yasak cihazların/programların kullanılması, tüzel kişilere yönelik tedbirlere, banka veya kredi kartlarının kötüye kullanılması gibi hususlarda oluşacak sorumluluklara da ayrıntılı olarak yer verilmiştir. Daha önce yürürlüğe girmiş kanunlara göre ele alınan farklılığın tüzel kişilere yönelik gerçekleştirilecek ihlâl durumunda uygulanacak tedbirler olduğu göze çarpmaktadır [59].

### **3713 Sayılı Terörle Mücadele Kanunu’nda Yapılan Değişiklik**

12 Nisan 1991 yılında yayımlanan Terörle Mücadele Kanunu’nda terörün tanımına, kapsamına, suça dair tüm süreçlere yer verilmiş; ülkemizin bağımsızlığına ve bölünmez bütünlüğüne kişi veya kişilere yönelik yapılması gereken tüm işlemler ele alınmıştır. 1991 yılında yürürlüğe giren Türk Ceza Kanunu’na dâhil edilen bilişim suçları ise Terörle Mücadele

Kanunu’nda gerçekleştirilen ve 2006 yılında yayımlanan değişiklikle “terör amacı ile işlenen suçlar” kapsamına girmiştir. Dijital dünyanın önlenemez genişlemesiyle ülke menfaatine zarar verecek her türlü kişi ve kişilerin bu alanda da yer aldığı gerçeği göz önüne alındığında yapılan değişikliğin ne denli önemli bir adım olduğu da göze çarpmaktadır. Kanun’un ilgili maddelerinde tanımlanan fiilerin, terör örgütü faaliyetleri amacıyla gerçekleştirilmesi durumunda siber ortamda da olsa terör suçlusu sayılacaktır. Bu durum, ülkemizde siber uzayın öneminin varlığı tam anlamıyla kabul edildiğini, terörizm faaliyetlerinin bu alanda da olabileceğinin yetkililerce de kabul edildiğini göstermektedir [60].

### **5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**

23 Mayıs 2007 tarihinde yürürlüğe giren Kanun, dijital ortamda içerik sağlayıcıların, yer sağlayıcıların, erişim sağlayıcıların ve kullanıcıların uyması zorunlu olan tüm kuralları içermektedir. Ulaştırma ve Altyapı Bakanlığı’nın koordinatörlüğünde ve Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı’nın başkanlığınca işletilecek olan Kanun, dijital ortamda yer alan tanımların, görev dağılımlarının, yükümlülüklerin, tüm sorumlukların ve işleyişin yer almasıyla siber güvenlik farkındalığının oluştuğunun ve politikaların ülkemizde uygulandığının en temel göstergesi olmuştur. Söz konusu kanunun yayımlanması ile Telekomünikasyon Kurumu’nda yürütme ve işletme sağlayacak bazı kadrolar ihdas edilmiştir. Kanun’da dijital ortamlarda gerçekleşecek ihlâl durumunda söz konusu ihlâl sebepleri olacak içeriklere erişim engeli getirme hakkı hâkim kararına bağlanmıştır. Bu durum kişinin özel hayatının korunması, mülkiyet hakkının korunması, haberleşme özgürlüğüne yönelik gerçekleştirilecek saldırılarda caydırıcılık hedeflenmiştir [61].

### **5809 Sayılı Elektronik Haberleşme Kanunu**

Türkiye’de siber güvenlik politika ve vizyonunun gelişmesinde bir diğer önemli adım da 5 Kasım 2018 tarihinde yayımlanan “5809 Sayılı Elektronik Haberleşme Kanunu”dur.

Elektronik Haberleşme Kanunu’nun yayımlanması ile dijital dünyada haberleşme faaliyetlerine hukuki anlamda geniş bir çerçeve getirilmiştir. Kanun’un temel amacı, elektronik haberleşme faaliyetlerinin yürütülmesinde düzenleme ve denetleme temelli rekabet sağlanması, üretici ve tüketicinin haklarının savunulmasıdır. Elektronik haberleşme hizmetlerinin ülkemizde genişlemesi, etkin bir şekilde verimli olarak kullanılması, şebeke ve alt yapı tesislerinin kurulmasına yönelik teşviklerin sağlanmasıdır. Bu anlamda usul, esas ve

tanımlamaların yer aldığı Kanun'un sorumluluğu Ulaştırma ve Altyapı Bakanlığı'na verilmiştir. Ayrıca elektronik haberleşme sektöründe yetkili merciler ve bu mercilerin görev ve sorumluluklarını da içermektedir. Kanun'un yayımlandığı ilk halinde sektöre yönelik usul ve esasların temel alınmış ancak 2014 ve 2016 yıllarında bazı hükümler eklenmesiyle Bilgi Teknolojileri ve İletişim Kurumu'na da siber güvenliğine yönelik Türkiye'nin politikalarını içerecek çerçevede sorumluluklar verilmiştir [62].

### **6698 Sayılı Kişisel Verilerin Korunması Kanunu**

24 Mart 2016 yılında yayımlanan “Kişisel Verilerin Korunması Kanunu” kişiselere ait özel verilerin işlenmesi konusunda ülkemizde gerçekleşmiş en büyük adımlardan biridir. Temelde anayasa ile korunan özel hayatın gizliliği prensibine dayanmakta olup temel hak ve hürriyetlerin korunması açısından önemli rol üstlenmiştir. 19 sayfadan oluşan ve detaylı olarak hazırlanmış Kanun gerçek ve tüzel kişilerin sorumluluklarını, uyulacak kuralları, usulleri, esasları belirlemeyi hedeflemiştir. Hak ihlâli durumunda nasıl ve nereye başvuru yapılacağı, bu anlamda oluşacak suçları içeren Kanun'un yayımlanması ile birlikte 30 Ocak 2017 tarihinde “Kişisel Verileri Koruma Kurumu” kurulmuştur. Bu kurum, kanun ve yasalarla teminat altına alınan kişisel verileri korumak amacıyla denetleyici ve düzenleyici sorumluluğundadır. 9 adet kurul üyesinden oluşmakta olup 5 üyenin atamasını Türkiye Büyük Millet Meclisi (TBMM), 4'ünün atamasını ise Cumhurbaşkanı yapmaktadır. Kuruma verilen görevler arasında:

- Yürürlükteki mevzuat ve uygulamaların takibinin yapılması,
  - Araştırma, inceleme, değerlendirme faaliyetlerinin sağlanması,
  - İhtiyaç hâsıl olduğu takdirde üniversitelerle, kamu kurumlarıyla, sivil toplum kuruluşlarıyla ve meslek kuruluşlarıyla iş birliği yapılması,
  - İlgili tüm konulardaki gelişmelerin takibi, değerlendirilmesi, iş birliği sağlanması ve toplantılara katılınması,
  - Yıllık olarak faaliyet raporu oluşturulması ve Cumhurbaşkanlığına, TBMM İnsan Haklarını İnceleme Komisyonu'na sunulması,
  - Kanunlar çerçevesinde verilebilecek tüm görevleri yapmak [63]
- yer almaktadır.

### 2.1.2. İlgili Çalışmalar

Shafqat ve diğ. (2016) çalışmalarında, belgelenmiş yasal, operasyonel, teknik ve politikayla ilgili önlemlere dayalı olarak yirmi ülkenin “Ulusal Siber Güvenlik Stratejileri”ni analiz etmekte ve karşılaştırmaktadır. Araştırmalarının sonucu olarak ulusal düzeyde siber güvenlik görevlerini yönetmek için resmi kurumların kurulması ve ulusal siber uzayı hedef alan siber saldırılarla mücadele için CERTS kurulması ihtiyacının gerekliliğini göstermiştir. Siber politikaların tam anlamıyla oluşturulmasında, siber farkındalık ve kapasite geliştirme programlarının amaçlarının, tanımlarının ve yasal önlemlerin tam olarak anlaşılması ve hayata uygulanması yatmaktadır. Karşılaştırmaya dayalı olarak gerçekleştirildikleri araştırmada, ulusal siber güvenlik ve dayanıklılık durumunu iyileştirmek için en iyi uygulamaları önermişler, siber güvenlik stratejilerini geliştirmeyi veya güncellemeyi planlayan ülkelerin çalışmalarını daha avantajlı nasıl kullanabileceklerini tanımlamışlardır [28].

Devlet savunmasının amacını temelde üniter devletin bütünlüğünü korumak ve her türlü olumsuzluktan kurtarmak olarak tanımlayan Rizal ve diğ. (2016) çalışmalarında Endonezya Cumhuriyeti'nin, devletin egemenliğinin yanı sıra askeri veya askeri olmayan her türlü tehdide karşı güvenliğinin sağlanmasına yönelik tedbirler üzerinde durmuşlardır. Ulusun egemenliğini ve güvenliğini potansiyel olarak tehdit eden siber saldırı tehdidinin hem devlet hem de devlet dışı aktörler tarafından başlatılabileceği ve bu saldırılardaki aktörlerin bir birey, bir grup insan, bir kuruluş, bir organizasyon ve hatta bir ülke olabileceğini vurgulayan yazarlar, hükümetin siber güvenlik stratejilerini formülize etmesini ve siber saldırılara karşı savunmak için kapsamlı adımlar belirleyerek siber tehditleri öngörmesi, hatta saldırıların türleri ve karşı önlemlerin ölçeği ile analiz edilerek hukuk kurallarının oluşturulması gerektiğini savunmuşlardır [29].

Modern zamanlarda siber uzayda güvenliğin sağlanması çoğu devlet için ulusal güvenliğin temel görevidir. Devletlerin siber güvenliğe ulusal güvenlik politikaları açısından farklı yaklaşımları vardır. Bu yaklaşımlar, siber güvenliği sivil bir faaliyet olarak görenler ve siber güvenliği ülke savunmasının temel faktörleri olarak görenler olmak üzere iki kategoriye ayrılabilir. Siber güvenlik politikalarının oluşturulmasında veya uygulanmasında siber savaşı askeri planlamalarına ve organizasyonlarına dahil eden devletler, siber saldırıları ulusal güvenliklerine yönelik bir tehdit olarak algılamak, sivil bir faaliyet olarak misyon edinmiş devletler, siber izinsiz girişleri yalnızca belirli sektörler için güvenlik riskleri olarak tanımlamaktadırlar. Tomic ve diğ. (2018) çalışmalarında, yukarıdaki hususları temel alarak siber güvenlik ve tehdit algılamalarına ve bunların kaynaklarına yönelik hem sivil hem de askeri

yaklaşımları teorize etmektedir. Ele alınan teorik çerçeve ile Doğu Avrupa ülkeleri ve Baltık Devletlerinin siber güvenlik politikaları temel olarak incelenmiştir [30].

Ticari, askeri ve istihbarat amacı ne olursa olsun, her türlü veri, bilgi ve bilgiye ulaşmanın birden fazla yolu bulunmakta olup bu durum bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasını gerektirmektedir. Siber istihbarat ve casusluk yöntemleri de giderek daha karmaşık hale gelmekte ve bazen ülkeler arasında sert tartışmaları ve çatışmaları ateşlemekte ve siber güvenlik politikasını uygulamanın her ülke için zorunluluk haline gelmesini tetiklemektedir. Bu nedenle gelişmiş ülkelerde olduğu gibi Asya Ülkelerinde de hükümetler, siber uzayda güvenliği sağlarken inovasyonu ve ekonomiyi artırmak için internet platformunun açıklığını sağlamak ve vatandaşlarının kişisel bilgilerini ve mahremiyetini kötüye kullanılmaktan korumak için siber güvenlik politikası ve mevzuatı uygulamışlardır. Bu bağlamda çeşitli önlemler ve eylemler geliştirilmiş ve yürürlüğe girmiştir. Sunkpho ve diğ. (2018) çalışmalarında, Endonezya, Malezya, Filipinler, Singapur, Tayland ve Vietnam dâhil olmak üzere 6 büyük Asya ülkesinin siber güvenlik politikalarına odaklanarak Asya ülkelerinde siber güvenlik ve veri korumasına ilişkin son yasal ve politik gelişmelere genel bir bakış sunmuşlardır. Çalışmada ayrıca, büyüyen siber tehditlerle mücadele etmek için Asya ülkeleri arasında daha fazla iş birliği yapılması önerilmiştir [31].

Bilgi ve iletişim teknolojilerini bir gelişim aracı olarak bilinçli olarak kullanılması, dijital bilgi sistemlerinin kullanımının artmasıyla sonuçlanmıştır. Özel ve kamu kuruluşlarında, toplumun genelinde bu dijital bilgi sistemleri, artan güvenlik açıklarını beraberinde getirmekte ve özellikle Kritik Ulusal Bilgi Altyapısına (Critical National Information Infrastructure-CNII) yönelik riskleri ve yanı sıra hacking, izinsiz giriş, kötü amaçlı kod ve DoS saldırıları gibi siber suçları da ortaya çıkarmaktadır. Malezya'nın siber güvenlik politikalarının üzerinde duran Hashim (2011) çalışmasında ülkenin e-egemenliğini tehlikeye atan siber tehditlerin büyümesini kabul eden bir siber güvenlik politikasının uygulanmış olduğunu ve bunun da Malezya'nın Ulusal Siber Güvenlik Politikası (NCSP), Kritik Ulusal Bilgi Altyapısı'nın karşılaşılan risklerle orantılı bir düzeyde korunmasını sağlamak için entegre bir şekilde yapılacak siber güvenlik uygulaması olduğunu belirtmişleridir. Devlet mekanizmaları eliyle yürütülen uygulamada, çeşitli bakanlıkları ve kurumları, sonunda istikrarı, sosyal refahı ve sosyal refahı teşvik edecek, güvenli, esnek ve kendine güvenen bir Kritik Ulusal Bilgi Altyapısı'na sahip olma vizyonunu karşılamak için birlikte çalışmaya çekmiştir. Uygulamanın başarıyla sağlandığını iddia eden yazar, Malezya'nın Kritik Ulusal Bilgi Altyapısı'nın, teknolojik ilerlemenin getirdiği zorlukları

ve fırsatları karşılamak için daha iyi bir konuma sahip olacağını ve 2020 yılı sonrasındaki hedeflere ulaşılmasında yardımcı olacağını belirtmiştir [32].

Hwang ve diğ. (2021) çalışmalarında, Kuzey Kore'ye yapılan siber terör saldırılarının amaçları, biçimleri, mevcut eğilimleri ve özelliklerinin niteliksel bir analizini yapmakta ve başarılı bir uluslararası politika müdahalesine doğru daha fazla ilerleme sağlamanın bir yolunu önerilmektedir. Uluslararası siyasi atmosferde son zamanlarda meydana gelen hızlı değişikliklere rağmen, Kuzey Kore'nin nükleer silahlar ve uzun menzilli balistik füzeler geliştirmesiyle uluslararası istikrar için bir tehdit oluşturduğunu iddia eden yazarlar siber saldırıların düşük maliyetler ile gerçekleşmesinin, siber terörizmi Kuzey Kore için çekici bir seçenek haline getirdiğine dikkat çekmiştir. Ayrıca çalışmada, uluslararası politika bağlamında siber terörizmin çok yönlü ve asimetrik doğasını ele alan Kuzey Kore siber terörizmine ilişkin daha kapsamlı bir görüş için kriminolojik çerçevelerden ve dünya siyasetinin ağ teorisinden perspektifler sunulmuştur [33].

Büyük ölçekli siber saldırılar dünya çapında endişe verici bir oranda artmakta ve genellikle geniş çapta duyurulan ve popüler hale getirilen siber terörizm tehdidiyle ilişkilendirilmektedir. Bu durumlarla birlikte, siber terörizmi yeni bir araştırma alanı olarak tanımlayan Plotnek ve diğ. (2021) çalışmalarında, 'siber terörizm' tanımının karşılaştırmalı bir analizini sunmakta ve evrensel olarak uygulanabilir yeni bir tanım ve sınıflandırma önermektedir. Sunulan yeni tanım, yeni önerilen sınıflandırmaya göre tanımlanan tüm temel ortak noktaları (yani aktör, güdü, niyet, araç, etki ve hedef) içeren, kamuya açık literatürdeki mevcut tanımların ayrıntılı analizlerinden türetilmiştir. Siber terörizmi tanımlamaya yönelik sunulan bu yeni yaklaşımda, küresel iş birliği ve araştırma için daha geniş bir tehdit hakkında ortak bir anlayış sağlamasını, siber terörizmin alt kümelerinin belirli yasal veya özel uygulamalar için tanımlanmasını önermişlerdir [34].

Broeders ve diğ. (2021) çalışmalarında, Birleşmiş Milletler (BM) Güvenlik Konseyi'nin daimî beş üyesi içinde ve genelinde siber terörizme ilişkin ulusal politikaların ve uluslararası diplomasinin ve siber normlara ilişkin BM sürecinin evrimini ve etkileşimini analiz etmişlerdir. Çalışmalarında ilk olarak, önleyici tedbirlerin düşük etkili siber faaliyetlere ve çevrimiçi içeriğe genişletilmesi yoluyla ulusal politikaların siber terörizmi bir bilgi güvenliği sorunu olarak aşamalı olarak nasıl dile getirdiğini ortaya koymuşlar. İkinci olarak, siber terörizm konusundaki diplomatik dilin kapsamlı ve kesin olmayan tanımların benimsenmesi yoluyla uluslararası alanda nasıl bir rol oynayabileceğini sorunsallaştırmışlardır. Üçüncü olarak ise, BM'nin diplomatik çabalarıyla, siber terörizm konusundaki normatif tartışmaları bilgi güvenliği

konusundaki tartışmalarla birleştiren yanlış bilgi operasyonlarını giderek daha fazla büyüdüğü, küresel olarak insan haklarını korumayı gerektirdiği sonucuna varmışlardır [35].

Terörizm, suç ve savaş tanıdık kavramlardır; ancak bunların siber uzay yoluyla nasıl değiştirildiği henüz tam olarak anlaşılmış değildir. UK'de terörizmin tehdit seviyesi orta seviyeye düşmüş olsa da, teknolojinin hayatımızdaki daha fazla gerekliliği ve varlığı nedeniyle, siber terörizmin oluşturduğu tehdit COVID pandemisi boyunca iyice artmıştır. Correia (2022) araştırmasında, ortak bir siber terörizm tanımı ve çerçevesinin gerekliliğini, ayrıca algıların neler olduğunu belirlemeyi amaçlamıştır. Siber terörizmin kabul edilmiş bir tanımının olmadığını ve ayrıca mevcut akademik tanımların UK mevzuatıyla uyumlu olmadığını, terörist faaliyetlerin siber etkin veya siber bağımlı olduğunu sınıflandıran bir siber terörizm çerçevesinin olmadığını vurgulamışlardır. Çalışmada, konuyla ilgili yanlış anlamalara ilişkin daha büyük sorunları temsil edebileceğinden, halkın siber terörizme yönelik algılarının ne olduğunu belirlemeyi amaçlayarak bir çevrimiçi anket düzenlenmiştir. Çevrimiçi anketten elde edilen veriler, UK'de örnek popülasyon arasında siber terörizme karşı tutulan görüşlerde bir miktar anlaşma olmasına rağmen, yine de genel halkın siber terörist faaliyetlerini belirleme ve bildirme yeteneği üzerinde etkileri olabilecek bazı yanlış anlamaların mevcut olduğunu tespit etmiştir. Genel olarak yapılan literatür taramasından ve birincil veri toplamadan elde edilen bulgular, UK yasal tanımlarıyla uyumlu bir siber terörizm tanımı geliştirmeye yardımcı olduğunu savunulmuştur [36].

Siber terörizm, tüm dünyanın bugünlerde karşı karşıya olduğu en büyük tehditlerden biridir. Terör yanlısı gruplar daha fazla destekçi ve sempatican kazanmak için siber uzaydan yararlanırken, bu durum ulusal güvenlik için ciddi bir tehdit haline gelmiştir. Bu duruma yönelik farkındalık yaratmak isteyen Tamerin (2021) ve diğ. çalışmalarında, Malezya Silahlı Kuvvetleri (Malaysian Armed Forces-MAF) personeli arasında siber terörizm ile ilgili farkındalık oluşturmak için “Siber Terörizm Sorunlarına Yönelik Karşı Anlatı Siber Güvenlik Modeli” adını verdikleri bir model sunmuşlardır. Önerilen model, siber terörizm modeliyle ilgili olarak ISO/IEC 27032:2012 standardına dayalı olarak oluşturulmuş; askeri BT uzmanlarına sorulmuş ve daha sonra bu yeni geliştirilmiş model doğrulanmıştır. Böyle bir model oluşturmanın çok önemli olduğu konusunda hemfikir olunmuştur; terörle mücadele çabaları için tam iş birliğine ihtiyaç duyulduğu vurgulanan bu çalışmanın nihai çıktısı, daha sonra ulusal savaş ilhamı doğrultusunda MAF ortamında potansiyel olarak uyarlanacak olan “Karşı Anlatı Bilgi Teknolojisi Modeli”dir [37].

Shandler ve diğ. (2021) çalışmalarında, siber terörizme maruz kalmanın misilleme amaçlı askeri saldırılara neden olup olmadığını, bunu hangi psikolojik mekanizmanın yaptığını vurgulamışlardır. Bir dizi kontrollü rastgele deney yoluyla yapılan bu çalışma, ABD, UK ve İsrail'deki kritik altyapılara yönelik siber ve geleneksel terör saldırılarını gösteren televizyon haber raporlarını analiz etmişlerdir. Elde edilen bulgular, yalnızca ölümcül siber terörizmin misilleme için güçlü desteği tetiklediğini göstermiştir. Siber terörizmin giderek artan uluslararası seviyeye çıkmasından endişe edilen çalışmada, bu tehdide maruz kalmanın, saldırının ölümcüllüğüne bağlı olarak misilleme politikaları için güçlü politika, teknik ve halk bilincinin desteği oluşturduğunu vurgulamışlardır [38].

Diorditsa ve diğ. (2021) çalışmalarında, siber terörizmi Ukrayna'nın siber güvenliğine yönelik bir tehdit olarak analiz etmişlerdir. Devlet çıkarlarına zarar vermeyi amaçlayan oldukça fazla sayıda terör eyleminin günümüzde hem gerçek dünyada hem de siber ortamda gerçekleştirilebilmesinden kaynaklanmaktadır. Haddi zatında eylemler bilgisayar sistemleri kullanılarak işlenir ve siber uzayda yapılır, yazarlar bu tür sosyal açıdan tehlikeli eylemleri “siber terörizm” olarak tanımlamayı önermişler. Çalışma, hukuk araştırmalarında doğrudan uygulanan bir dizi felsefî, genel, bilimsel ve diğer yöntemlerin bir incelemesidir. Yazarlar terimleri yorumlayarak, araştırma konusunun kavramsal ve kategorik ayrımını oluşturmuşlardır. Bilgi terörizmi ile siber terörizm arasındaki farkı anlatarak, devletin bilgi güvenliği alanındaki zorluklara karşı hızlı tepki verebilecek bir Siber Komutanlık'ın oluşturulması gerekliliğine vurgu yapılmıştır [39].

Körfez İşbirliği Konseyi (Gulf Cooperation Council-GCC), petrol ve gaz endüstrisinin yaygınlığı ve daha yakın zamanda dijital ekonomiye yapılan önemli yatırımlar nedeniyle dünyanın en hızlı büyüyen ekonomilerinden bazılarını içeren Arap Devletlerinin siyasi ve ekonomik bir birliğidir. Bununla birlikte, son yıllarda, siber suç ve siber tehdit oranları önemli ölçüde artarak bölgenin güvenliğine ve ekonomik performansına yönelik zorluklar ortaya çıkarmıştır. Alshabib ve diğ. (2021) çalışmalarında, ulusötesi işbirliğine girme gerekliliği kapsamında bölgedeki siber güvenlik tehditleri, stratejik işbirliği sorunları ve siber suç ve siber güvenlik alanlarındaki ortak zorlukların üstesinden gelmek için bir analiz sunmaktadır. Çalışmada, siber güvenlik politikasının belirli yönleri tartışılmaktadır, önleyici ve hafifletici eylemler tanımlanmakta, potansiyel bölge içi ve uluslararası işbirliği yolları gösterilmekte ve siber güvenlik yeteneklerini ve direncini artırmak için etkili stratejinin bir formülasyonu sağlanmaktadır [40].

Terör, ülkeler için büyük bir tehdit oluşturmaya devam etmekte ve uluslararası barış ve güvenliğin temelini baltalamaktadır. Nijerya, ülke içinde yerinden edilmiş kişiler ve ekonomik ve sosyal kalkınma için son derece olumsuz sonuçlara sebep olan çeşitli terörist grupların ortaya koyduğu birçok zorlukla karşı karşıya kalmaya devam etmektedir. Abiodun (2021) çalışmasında Nijerya'da siber terörizmin kriminalize edilmesinin yasal çerçevesini oluşturan maddeleri, İngiltere ve ABD'dekilerle karşılaştırmalı olarak incelemektedir. Çalışmada, mevzuatın yeterliliğini sorgulamak amacıyla farklı yargı alanlarındaki yasal çerçeveyi karşılaştıran karşılaştırmalı bir analiz yöntemi ile ele alınmıştır. Ayrıca mevcut yasalardaki boşlukları değerlendirmeye ve/veya belirlemeye çalışılmaktadır. Makalede, hem ulusal hem de uluslararası toplulukların hukuki tepkileri de analiz edilmektedir. Gerçekleştirilen analizde, Nijerya'da terör saldırılarının yeniden ortaya çıkmasıyla, Nijerya'daki siber terör saldırıları yakın olduğu için sadece bir yasanın çıkarılmasının yeterli olmayabileceğini ortaya koymuştur. Yazar, Ulusal Siber Nijerya'da siber güvenlik için gidilecek merkez olacak ve Nijerya'daki tüm devlet kurumları ve diğer kurumlar için siber istihbarat entegrasyonunu kolaylaştıracak ortak bir görev gücünün ve Komuta Merkezi'nin kurulmasının gerekliliğine dikkat çekmiştir [41].

1990'lu yılların başlamasıyla birlikte ABD ve Rusya Federasyonu arasında yaşanan Soğuk Savaş döneminde gerçekleşen askeri ve siyasi rekabet kapsamında geliştirilen ağ teknolojileri temelli yeniliklerin sivil kullanıma açılmasıyla siber uzay denilen alanın ortaya çıkışı başlamıştır. Soğuk Savaş Dönemi'nin bitmesiyle dünyada birçok gelişme yaşanmış, bilgi çağı olma yolunda teknoloji gelişmeleri tavan yapmıştır. 2000'lerin ilk 10 yılından sonra özellikle mobil teknolojilerin ve mobil cihazların yaygınlaşmasıyla akıllı telefonlar ve birlikte sosyal medya uygulamaları güncel yaşamın asla vazgeçilemeyen birer ögesi olmuşlardır. Vazgeçilmeyen teknoloji de kara, deniz, hava, uzay ile birlikte siber uzay kavramının doğmasına sebep olmuştur. Türkiye'de de 1990'lı yılların ilerlemesiyle teknoloji daha da yayılmış, ilerleyen teknoloji ile birlikte siber güvenlik alanının önemi ve bu alanda yapılan çalışmalar artmaya başlamıştır. Bu yaşanan süreçler ise dünya ile paralel olarak 2000'li yılların sonrasında hızlandırılmıştır. Bu kapsamda Darıcılı (2019) yaptığı çalışmada, Türkiye'nin sahip olduğu siber güvenlik politikalarını ve bu alanda gerçekleşen kurumsal planlamaların irdelenmesini ve bunu temel alarak değerlendirilmesini sağlamıştır. Türkiye'nin güçlü, etkin bir siber savunma ve saldırı altyapısına sahip olması amacıyla, dünyada bu alanda çalışan diğer devletlerin siber güvenlik politikaları ile ilgili planlamaları analiz edilmiştir. Ayrıca çalışmada, reel politik güvenlik paradigmalarına uygun şekilde, devlet merkezli bir yaklaşımla öneriler ortaya konulmaya çalışılmıştır [42].

Siber ortamlardaki dijital verilerin katlanarak artmasıyla birlikte güvenlik önlemleri daha fazla önem kazanmıştır. Siber güvenlik tehditleri ulusal ve uluslararası birimler tarafından ortaya çıkarılmakta ve bu tehditlerin sayısı her geçen gün artmaktadır. Siber güvenlik risklerinin ortadan kaldırılması, etkin bir siber güvenlik stratejisi ile mümkündür. Yönetim kavramı yeterli olmadığı için bu stratejinin uygulanması tüm paydaşları yönetim süreçlerine dâhil eden siber yönetim ile mümkündür. Savaş ve diğ. (2022) çalışmada, siber güvenliğin sağlanmasında siber yönetişimin önemi ve gerekliliğini vurgulamaktadır. Çalışmada, siber güvenlik yönetişimi için yapılan araştırmalar ve sonuçları incelenmiştir. Bu amaçla betimsel bir araştırma modeli kullanılmıştır. Araştırma felsefesi açısından uygulama yöntemine ilişkin temel araştırma modeli ve belgesel araştırma modeli oluşturulmuştur. Araştırmanın kapsamını “Web of Science, EBSCO, Scopus, Google Scholar ve TR Index”ten elde edilen çalışmalar oluşturmaktadır. Çalışmaya göre son 5 yılda yapılan araştırmalar, belirlenen anahtar kelimelerle indirilmiş; elde edilen sonuç, farklı ülkelerde siber güvenlik yönetişimi için yerel çözümler üreten çalışmalar olmasına rağmen henüz genel bir yönetim çerçevesinin oluşturulmadığını göstermiştir [43].

Siber güvenlik, teknolojik gelişmeler ile temel bilgi teknolojileri ve ağ sistemlerinin yanında hayatın her alanında ve özellikle iletişim, ulaşım, gıda üretim, enerji, finans, su ve altyapı gibi toplumlar için en önemli sistemlerine yönelik de bir kavram haline gelmiştir. Özellikle bir ulusun güvenliğinin sağlanması, kritik altyapılarının korunması ve siber güvenlik politikalarının oluşturulması noktasında farkındalık kazanmışlardır. Bu açıdan bakıldığında zaman siber güvenliği her ulus için bir kamu politikası konusu olarak değerlendirmek ve hükümetlerin kamu politikası yaklaşımları bazında ele almak gerekmektedir. Göçoğlu (2018) yapmış olduğu tez çalışmada ilk olarak bir örnek olay üzerinden ve 5 farklı ülkeye bakarak gerçekleştirdiği inceleme sonucuyla siber güvenlik ve kamu politikaları arasında yadsınamaz ilişkiyi belirtmiştir. Türkiye’nin kalkınma hedefleri, sahip olduğu strateji, hukuki ve eylem belgeleri, raporlar gibi ve siber güvenlik politikalarını tanımlayan 28 adet resmi belge içerikleri araştırma kapsamına alınmış, “NVivo 11” adı verilen nitel veri analiz programı ile analiz edilmiş ve incelenmiştir. Yazarın yapmış olduğu çalışmada, Türkiye’nin siber savunma, kritik altyapı politikaları, karar verme modelleri, kamu politikası analizi yaklaşımları ve üretilen politikaların özellikleri birbirleriyle ilişkili bir şekilde ortaya konulmuştur [44].

Siber ortamların kullanımı, özellikle internet ve sosyal medyanın yaygınlaşmasıyla birlikte siber ortamlardaki tehditler de artmış ve bu ortamlardan hem kurumlar hem de bireyler zarar görmektedir. Bu zararın bazen maddi olabileceği gibi manevi de olabilir. Tüm bu

gelişmeler ve olumsuz faktörler göz önüne alındığında, gerçek hayatta yönetim mekanizmaları olduğu gibi siber ortamlarda da yönetim mekanizmaları kurma ihtiyacı ortaya çıkmıştır.

Kurulacak yönetim mekanizmaları sadece donanım teknolojileri ve yapıları ile ilgili olmayacak, siber ortamların yönetimi için ulusal ve uluslararası standartların belirlendiği politika ve stratejilerden oluşmalıdır. Bir yönetim modeli oluşturulmalı; kurumlar arasında, uluslararasıda tüm paydaşların dâhil olduğu çok yönlü çalışmalar yapılmalıdır.

Bu çalışmalar kapsamında gerçekleştirilen ve siber yönetişim kavramının bir alt kümesi olarak tanımlanabilecek “Siber Güvenlik Yaklaşımı” üzerine yapılan araştırma da dünya gündeminin bu yönetişim konusuna giderek daha fazla ağırlık verdiğini ancak henüz yeterli düzeyde olmadığını göstermiştir. Çalışmalarda politika bütünlüğüne ihtiyaç olduğu, belirli çözümler yerine dünya çapında geçerli kuralların ve stratejilerin oluşturulması gerektiği sonucuna ulaşılmaktadır.

Siber güvenlik çalışmaları ve politikalarının oluşturulmasında dünyanın farklı ülkelerinde yerel çözümler üreten çalışmalar olmasına rağmen henüz genel bir çerçevesinin oluşturulmadığı görülmektedir. Ayrıca teknolojide ve ticarete gelişmiş ülkelerin başında gelen ABD ve Çin gibi devletlerin siber uzayın yönetimine ve siber güvenlik alanında yaptığı çalışmalara karşı görünmez bir mücadele içinde oldukları da ortaya çıkmıştır.

Siber güvenlik politikalarının hazırlanması ve farkındalık oluşturulması hususunun kamu, özel sektör ve bireysel kullanıcılar dâhil olmak üzere bir ağı erişimi olan tüm bireyleri ve kuruluşları ilgilendirmektedir. İnsanların, kurumların ve ulusların yaşadıkları fiziksel ortamda güvenlik hususunu önemsedikleri gibi bilgi ve iletişim ortamlarında da güvenlik hususlarına önem vermelidirler.

Bu korunmanın ilk adımı, üreticinin geliştirdiği teknolojik donanımda bir boşluk bırakmaması, erişilmemesi gereken bilgilere yetkisiz erişimin kapısını açmamasıdır. Yöneticiler de belirlenecek ve uygulanacak politikalara güvenlik zafiyeti oluşturacak kararlara imza atmamalıdır. Kullanıcılar, kişisel siber güvenliğini sağlamalı, bir firma tarafından gerekli eğitimleri almalı ve alınan önlemlere titizlikle uymalıdır. Belirlenen politikaların siber ortamlarda mevcut tüm kurum, kuruluş, kişi ve cihazlar için geçerli olması gerekmektedir. Siber ortamları oluşturan unsurların içerisinde tüm kişi, kurum ve cihazlar yer aldığından, onları bir araya getiren politikaların genel olması gerekmektedir.

Tüm kurum, kişi ve cihazlar için ortak kuralların uygulanması gerekmektedir. Yayınlanacak politikalar, rehberler, stratejiler uluslararası nitelikte olmalıdır. Çalışmaların öncelikle ulusal olması tüm kişi, kurum ve kuruluşları kapsamı daha sonra şehir veya sektör

özelinde yapılması gerekmektedir. Bu nedenle, ülke veya kurum temelli bir yaklaşım yerine, özellikle dünya çapında politika yapıcı kurumların devreye girmesi ve tüm dünya tarafından kabul edilen diğer standartlar gibi politikaları belirlemesi gerekmektedir.

Belirlenen politikaların, siber ortamların farklı konularına göre ayarlanabilir olması gerekmektedir. Örneğin bulut bilişim alanındaki çalışmalar ve politikalar nesnelerin interneti konusuna da kolayca uyarlanabilmelidir. Siber ortamlardaki bileşenlerin sayısı sürekli artmakta ve bu nedenle sürekli yeni alt küme alanları oluşturulmaktadır. Hızla gelişen dijital dünyada, politikaları sık sık güncellemek yerine, siber ortamlarda daha ileri görüşlü, daha kapsamlı ve alt kümelere uyarlanabilir politikalar hazırlamak gerekmektedir.

Aynı şekilde belirlenen politikaların da hiyerarşik bir yapıya sahip olması gerekmektedir. Genel olarak özel sektöre inildikçe daralan bir yapıda tasarlanmalı ve tüm alt alanların ihtiyaçlarına da uyum sağlamalıdır. Politikaların ve planların hazırlanması aşamasında oldukça fazla sayıda kamu kurumu, özel sektör ve bireysel kullanıcı ile görüşülmeli toplantı, seminer, çalıştay vb. faaliyetlere de katılımlarının sağlanması gerekmektedir.

Günümüzde önemli sosyal medya sitelerinin kullanıcı sayısının bile yüz milyonlarca olarak ifade edilmesi siber ortamlardaki yaşam boyutunu örneklendirebilir. İnternet kullanımına Nesnelerin İnterneti (Internet of Things-IoT), yapay zekâ, metaverse, robotik uygulamalar, mobil teknolojiler, bulut bilişim gibi birçok yenilikçi teknoloji eklendiğinde siber uzayın boyutları konusunda zihnin sınırlarını zorlayacak bir kapsam ortaya çıkacaktır.

Tarih boyunca devletler arasında hatta aynı milletin devletleri arasında süregelen mücadeleler olduğu gibi, bu ortamlardaki yönetim ve yönetişim mücadelesi de varlığını sürdürmektedir. Burada görünmez bir üstünlük mücadelesi var olmuştur ve bunun sonuçları tüm kullanıcıları etkileyecek bunun yanı sıra kritik altyapılara yapılan saldırılar teknolojik herhangi bir cihaz ya da sistem kullanıcısı olmayan insanları bile etkileyecektir.

Hayatın vazgeçilmez bir alanı olan siber ortamlarda iş ve işlemlerin güvenli bir şekilde yürütülmesi, kurumların kurulması ve yaşamın sürdürülmesi için ortak bir anlayış ve yönetim çerçevesine ihtiyaç vardır. Bu çerçeve yalnızca, bireyler, kurumlar veya devletler tarafından belirlenebilecek bir çerçeve değildir. Dünyanın düzenleyici ve bağlayıcı uluslararası kuruluşlarının desteğine ihtiyaç vardır. Elbette bu kurumların kendi başlarına belirleyecekleri politikalar genel olarak geçerli olmakla birlikte teknik bir yetersizlik de söz konusu olabilecektir.

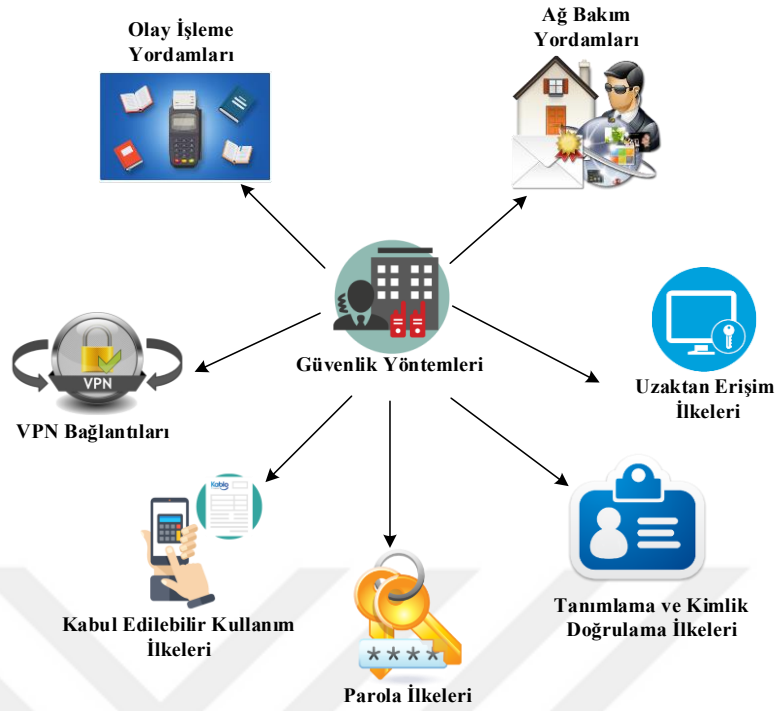
Stratejik, operasyonel ve taktik düzeylerde gösterilen faaliyetler belirlenerek iyi bir siber güvenlik stratejisi uygulanabilecektir. Türkiye, siber güvenlik stratejilerinin genişletilmesi ve

son yıllarda yaşanan ekonomik, teknolojik ve siyasi değişimler, küresel terör olayları ile tanımı değişen tehdit ve savaş alanında güçlü olabilmesi için, siber sorunları kurumlar, özel sektör ve mevcut yasaların/yönetmeliklerin yeniden değerlendirilmesi ile ele almalıdır.

Savaş alanının tanımı eskisi gibi değildir. Önümüzdeki on yılda siber dünyanın, güvenlik için en büyük tehditlerden biri olacağı kuşkusuzdur. Siber savaş, çatışan grupların ve ülkelerin bilgi sistemleri arasında gerçekleşebilir. Gelişmiş ülkeler siber tehditlerin farkındadır ve hâlihazırda siber savaş altyapısına yönelik çalışmalara ve saldırılara başlamışlardır. Siber savaş, teknolojinin her alanında yaşanmaktadır. Bu bağlamda, kritik bilgi sistemlerini ve kritik fiziksel altyapıyı içerenler de dâhil olmak üzere bir siber savunma hattı ve anlayışı geliştirilmelidir. Güçlü bir siber savunma elde etmek için en önemli adımın, bir strateji ve uygun bir siber savunma yapısı ortaya koymak olduğu unutulmamalıdır.

## **2.2. KRİTİK YAPILARDA GÜVENLİK BİLGİLERİ VE OLAY YÖNETİMİ**

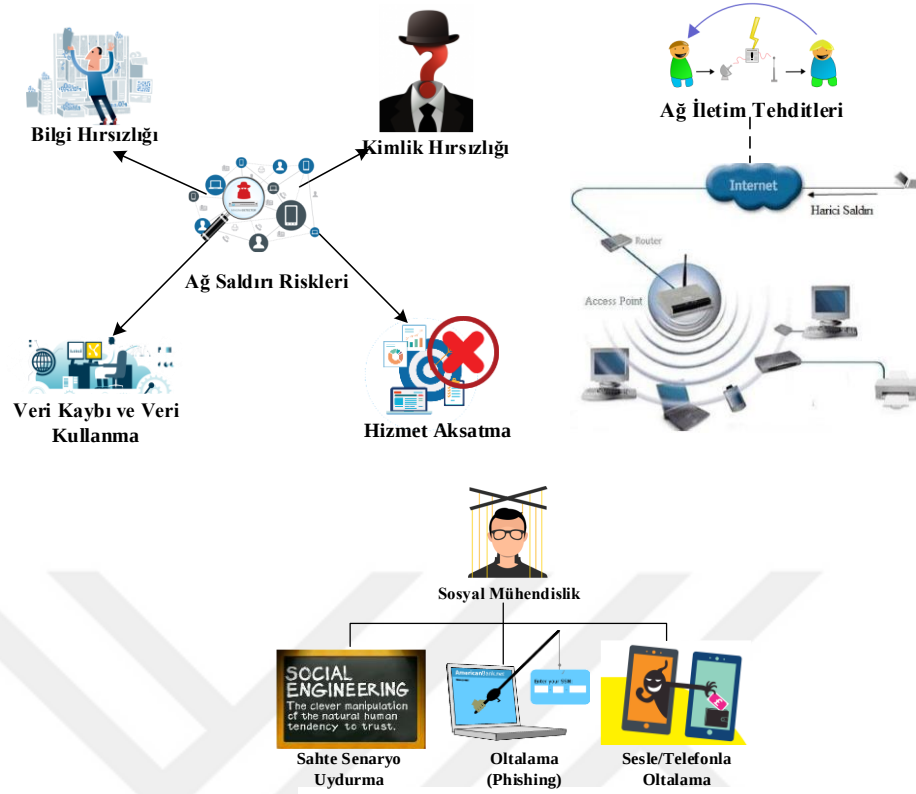
İnternetin hızla büyümesi ve daha yaygın ve erişilebilir hale gelmesinden itibaren internete bağlanan kişi ve cihazlar önemli ölçüde artmıştır. Kullanılabilirlik arttıkça internete erişim oranları artmış ve farklı özelliklere sahip farklı insan profilleri de internete bağlanmaya başlamıştır. Kişisel kullanıcılar, ticari kullanıcılar, devlet kurumları, her türlü kuruluş ve eğitim kurumunun kullanıcıları bu profillerden bazılarıdır. İnternetin gelişmesi ve kullanımının artması insanları daha yakın ve bağlı olmaya yöneltmiştir. Oluşan yakınlık ve bağlılık gitgide karmaşıklaştıran ve güvenlik ihtiyacı oluşan sanal bağlılıktan öteye gidememiştir. Ancak bilgi paylaşımı ve veri dağıtımını kolaylaşmaya başlamıştır. Bu durum bilgi güvenliği dünyasında da bir takım bağlılıklara evrilmiştir. Kullanıcı insan profillerinin birbirleri arasında güvenliklerine yönelik oluşturdıkları tehditler önemli ölçüde yükselmiş ve saldırılar daha karmaşık olmaya başlamıştır. Şekil 2.2’de güvenlik yöntem değerlendirmesine yer verilmiştir.



**Şekil 2.2:** Güvenlik yöntem değerlendirme

Ayrıca son yıllarda bilgi güvenliğine yönelik tehditler, dünyada aktif olarak kullanılan hizmetlere yönelik istismarların ve tehditlerin şirketler için bir kâr modeli haline gelmesi nedeniyle daha hedef odaklı ve sofistike bir hale gelmiştir. İstismarlar ve taviz verme teknikleri daha karmaşık ve detaylı hale gelirken, günlük erişim kayıtlarının analizi ile tehdit izleme, bilgi güvenliğinin önemli bir faktörü haline gelmiştir. Güvenlik bilgileri ve olay yönetimi (Security Information and Event Management-SIEM) anlamına gelmektedir ve ağ ve güvenlik cihazlarından veri toplama ve analiz etme yeteneklerine sahiptir. SIEM, günümüzde birçok Siber Güvenlik Operasyon Merkezi'nin kullandığı izleme yeteneklerini geliştirmek için çeşitli güvenlik cihazlarından gelen olayları ilişkilendirmek için tüm önemli bilgileri birleştirilmiş bir çerçevede toplamak için kullanılan bir yöntemdir. SIEM, ağ cihazlarından, sunuculardan, etki alanı denetleyicilerinden ve daha fazlasından güvenlik verilerini toplamaktadır; verilerdeki eğilimleri, tehditleri tespit etmek ve kullanıcıların uyarıları araştırmasını sağlamak için bu verileri depolayıp normalleştirmekte ve bu verilere analitik yöntemler uygulamaktadır.

SIEM, bir olay müdahale ekibine güvenlik olayları hakkında raporlama imkânı veren ve belirli bir kural kümesiyle eşleşen ve bir güvenlik sorununu uyarılarla belirten, veri toplayıcı, izleyici ve raporlama sistemidir. SIEM temelde bilgi güvenliğinin sağlanmasına yönelik çalışmakta olup temel amacı: Gizlilik, Bütünlük ve Kullanılabilirlik ilkerinin korunmasıdır.



Şekil 2.3: Güvenlik zafiyet türleri

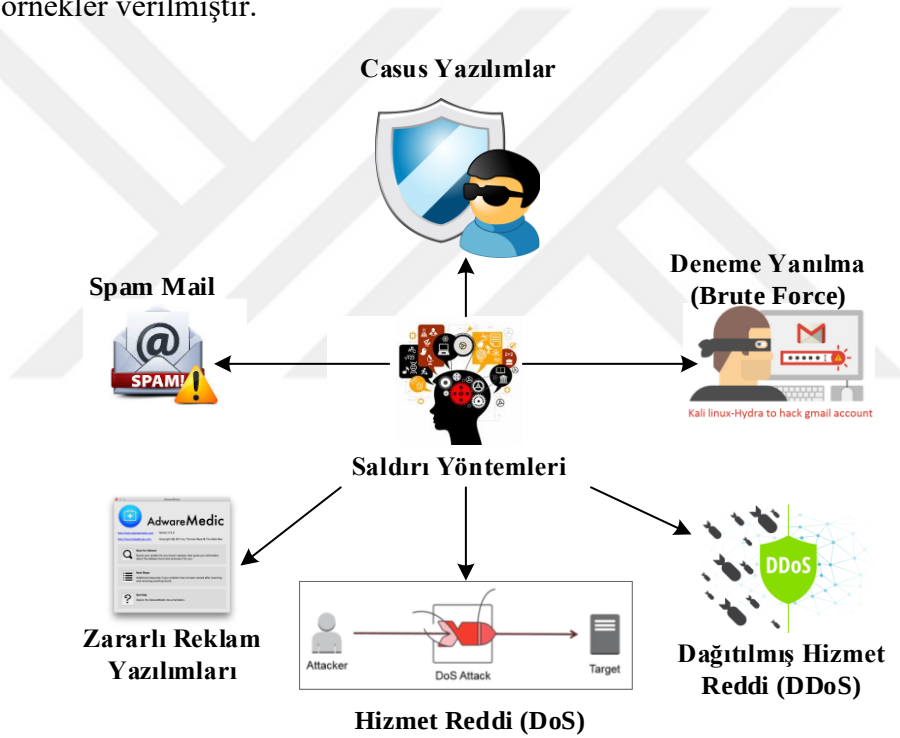
**Gizlilik:** bilginin değeri olduğu için yetkisiz üçüncü şahıslardan korunması anlamına gelmektedir. Bu değer bazen banka hesapları, kimlik numaraları, kredi kartı numaraları ve hatta devlet sırları olabilmektedir. Bu değerli verilerin korunması, bilgi güvenliğinin her şeyden önce var olmasının temel nedenidir. Gizlilik denilince akla ilk gelen şifrelemedir. Verilere yalnızca yetkili personelin veya üçüncü kişilerin erişebilmesini sağlamak buradaki en temel husustur. Dosya izinlerine sahip olmak ve bunları uygulamak, hassas verilere erişimi kısıtlamak amacıyla gizliliği sağlamak için internet üzerinden iletişim için bir güvenlik protokolü olan SSL/TLS (Güvenli Soket Katmanı-Secure Sockets Layer/ Taşıma Katmanı Güvenliği-Transport Layer Security) gibi örneklerle günümüz dünyasında yaygın çözümler kullanılmaktadır.

**Bütünlük:** bilginin bütünlüğü ise, bilgilerin değiştirilmesinden korunması anlamına gelmektedir. Bütünlük sağlanması için, verilerin doğru tutulması her anlamda önemlidir. Bütünlüğü sağlamak adına yaygın olan yöntemler arasında zaman damgaları kullanılarak alınan verilerin hash edilmesi ve orijinal mesajın hash değeri ile karşılaştırılması önemli örneklerden sayılmaktadır.

**Erişilebilirlik:** yetkili kişilerin gerektiğinde bilgiye ulaşabilmesi anlamına gelmektedir ve gerektiğinde bilgiye doğru kişiler erişemiyorsa bu bilginin hiçbir değeri yoktur.

Erişilebilirlik kuralını aşmak için yapılan DDoS saldırıları erişilbilirliğe kasteden ve günümüzde yaygın olarak kullanılan bir saldırı türüdür.

SIEM yazılımları, bir kuruluşun uygulamaları, güvenlik cihazları ve ana bilgisayar sistemleri tarafından oluşturulan günlük ve olay verilerini toplayarak ve bunları tek bir merkezi platformda bir araya getirerek çalışmaktadır. Bahze konu yazılımlar, yukarıda bahsedilen temel prensiplere gerçekleştirilen müdahaleleri de tespit etmeyi amaçlamaktadır. Virüsten koruma olaylarından, güvenlik duvarı günlüklerinden ve diğer konumlardan veri toplayıp; bu verileri kötü amaçlı yazılım etkinliği, başarısız ve başarılı oturum açma işlemleri şeklinde kategorilere ayırmaktadır. SIEM, ağ güvenliği izleme yoluyla bir tehdit belirlediğinde, bir uyarı oluşturur ve önceden belirlenmiş kurallara göre bir tehdit düzeyi tanımlar. Şekil 2.4'te güvenlik zafiyet türlerine örnekler verilmiştir.



Şekil 2.4: Güvenlik zafiyet türleri

SIEM araçları incelendiğinde birçok zafiyet türü göz çarpmaktadır. Örneğin, 10 dakikada 10 kez bir hesaba giriş yapmaya çalışan biri sorun olarak görülmemekte ancak 10 dakikada 100 kez gelen erişim isteği saldırı girişimi olarak işaretlenebilmektedir. SIEM, bu şekilde tehditleri algılamakta ve güvenlik uyarıları oluşturmaktadır. SIEM'in özel gösterge panoları ve olay yönetim sistemi, araştırma verimliliğini artırmakta ve yanlış pozitiflerle harcanan zamanı azaltmaktadır. SIEM, bir araya getirildiğinde ve entegre edildiğinde kuruluşlar için kapsamlı koruma sağlayan bir dizi yeteneğe sahiptir. Aynı zamanda tek bir

gösterge panosunda bir araya getirilerek daha kolay ve daha verimli bir yönetim imkânı sağlamaktadır. Bu alanda kullanılan yazılımlar, güvenlik ekiplerinin saldırgan taktiklerine, tekniklerine ve prosedürlerine ve bilinen güvenlik açığı göstergelerine ilişkin bilgilerden elde edilen tehdit kurallarıyla saldırgan içgörülerini elde etmesine olanak tanımaktadır. Bu, bir tehdide işaret edebilecek anormal davranışları izlemek için davranışları ve etkinlikleri analiz eden Kullanıcı ve Varlık Davranışı Analitiğini (User And Entity Behavior Analytics-UEBA) içerebilmektedir. Ayrıca davranış anormalliklerini, yanal hareketi ve güvenliği ihlal edilmiş hesapları da tespit edebilecektir.

Bu, daha önce görülmemiş tehditler için bilgi avı elde etmek için verilerdeki anormallikleri tespit eden güvenlik analitiği bileşenine benzemektedir. Yönetilen kurallar bileşeni, kuruluşların analistlerin neredeyse gerçek zamanlı güncellemeleriyle en son saldırgan tekniklerine neredeyse gerçek zamanlı olarak tepki vermesini sağlamaktadır. SIEM yazılımı bir tehdit, güvenlik açığı, saldırı veya şüpheli davranış belirlediğinde, hızlı yanıt için bir kuruluşun güvenlik ekipleri için uyarılar oluşturmaktadır. Yazılımın bazı sürümleri, aramalar ve gerçekleştirilecek eylemlerle birlikte otomatik olarak oluşturulan adım adım araştırma talimatlarını kullanarak araştırmaları hızlandırmak için iş akışı ve vaka yönetimi içermektedir. SIEM uyarıları ayrıca kullanıcı ihtiyaçlarına göre günlük yönetimi içinde özelleştirilebilir. Günlük yönetimi ise, SIEM'in üç ana alandan oluşan karmaşık bir bileşenidir:

**Veri toplama:** çeşitli uygulamalardan ve veri tabanlarından büyük miktarda veriyi tek bir yerde toplamak anlamına gelmektedir. SIEM, bir organizasyonun tüm ağındaki geniş bir kaynak yelpazesinden olay verilerini yakalamaktadır. Kullanıcılar, uygulamalar, varlıklar, bulut ortamları ve ağlardan gelen günlükler ve akış verileri gerçek zamanlı olarak toplanır, depolanır ve analiz edilir, bu da BT ve güvenlik ekiplerine ağlarının olay günlüğünü ve ağ akışı verilerini tek bir merkezi konumda otomatik olarak yönetme yeteneği vermektedir. Bazı SIEM çözümleri, dahili güvenlik verilerini önceden tanınan tehdit imzaları ve profilleriyle ilişkilendirmek için üçüncü taraf tehdit istihbaratı akışlarıyla da entegre olmakta; gerçek zamanlı tehdit akışlarıyla entegrasyon, ekiplerin yeni tür saldırı imzalarını engellemesini veya algılamasını sağlamaktadır.

**Veri normalleştirme:** SIEM, tüm farklı verilerin karşılaştırılmasına, ilişkilendirilmesine ve analiz edilmesine olanak tanımlanmaktadır. SIEM teknolojisinin ağda algılanan anormal davranışları sınıflandırırken tüm bağlı kullanıcılar, cihazlar ve uygulamalar genelinde güvenlik olaylarını izlemesini sağlamaktadır.

**Veri analizi/güvenlik olayı korelasyonu:** Bir veri ihlali, tehdit, saldırı veya güvenlik açığının olası belirtilerinin belirlenmesi anlamına gelmektedir. Olay korelasyonu, herhangi bir SIEM çözümünün önemli bir parçasıdır. Karmaşık veri modellerini belirlemek ve anlamak için gelişmiş analitiği kullanan olay korelasyonu, iş güvenliğine yönelik potansiyel tehditleri hızla bulmak ve azaltmak için iç görüler sağlamaktadır. Yöneticiler, özelleştirilebilir önceden tanımlanmış korelasyon kurallarını kullanarak, anında uyarılmakta ve daha önemli güvenlik sorunlarına dönüşmeden önce bunu azaltmak için uygun önlemleri alabilmektedir.

SIEM çözümleri, güvenlik olaylarının derinlemesine analiziyle ilişkili manuel iş akışlarını devre dışı bırakarak BT güvenlik ekipleri için Ortalama Algılama Süresi (Mean Time to Detect-MTTD)'ni ve Ortalama Yanıtlama Süresi (Mean Time to Response-MTTR) önemli ölçüde iyileştirmektedir. SIEM çözümleri, farklı yasal uyumluluk biçimlerine tabi olan kuruluşlar için popüler bir seçimdir. Sağladığı otomatik veri toplama ve analizi nedeniyle SIEM, tüm iş altyapısı genelinde uyumluluk verilerini toplamak ve doğrulamak için önemli bir araçtır.

Siber güvenlik ortamının ne kadar hızlı değiştiği göz önüne alındığında, kuruluşların hem bilinen hem de bilinmeyen güvenlik tehditlerini algılayabilen ve bunlara yanıt verebilen çözümlere güvenebilmesi gerekmektedir ve bu noktada SIEM ürünleri kullanmak veya kendi yazılımını kurumun geliştirmesi gerekli olmaktadır [16-23].

### 2.3. VERİ SETİ İLE İLGİLİ ÇALIŞMALAR

Bilgisayar ağları; güvenlik açıkları nedeniyle gün geçtikçe daha fazla ve farklı türlerde siber saldırıya maruz kalmaktadır. Bu nedenle siber güvenlik, herhangi bir şüpheli etkinliği tespit etmek için savunma sistemleri sunarak ağları mümkün olduğunca güvenli hale getirmeye çalışmaktadır. Bununla birlikte, ağ üzerinde konumlandırılmış güvenlik duvarları ve klasik STS, siber tehditleri tespit etmek için tanımlanmış veri tabanlarının sürekli güncellenmesinden dolayı tam anlamıyla bir güvenlik sağlayamamaktadır. Bu sebeple STS'lerin yeni yönergeleri, daha yüksek sayıda tespit oranlarına ve daha düşük yanlış alarm oranlarına sahip güvenilir sistemler tasarlamak için Makine Öğrenimi (ML) modellerinden yararlanmayı amaçlamaktadır. Bu yaklaşımı temel alan Moualla ve diğ. (2021) çalışmalarında UNSW-NB15 veri kümesinde ML tabanlı ağ saldırı tespit sistemlerinin performansını iyileştirmeye yönelik bir yaklaşım önermişlerdir. Ağ güvenliğinde önemli bir rol oynayan ve UNSW-NB15 veri kümesini kullanan çalışmaları göz önünde bulundurarak yeni bir ağ STS tanımlamışlardır. Önerilen sistem, dinamik olarak ölçeklenebilir çok sınıflı makine öğrenimi tabanlı bir ağ STS'dir.

Çalışmada, veri setindeki dengesiz sınıflar problemini çözmek için Sentetik Azınlık Aşırı Örneklemeye Tekniği (SMOTE) yöntemi kullanılmış ve daha sonra Aşırı Rastgele Ağaçlar Sınıflandırıcısı (Extremely Randomized Trees Classifier) kullanarak Gini Impurity kriteri ile veri setinde bulunan her sınıf için önemli özellikleri seçilmiştir. Önceden eğitilmiş bir Aşırı Öğrenme Makinesi (Extreme Learning Machines-ELM) modeli ile saldırıların her biri için ikili bir sınıflandırıcı olarak “One-versus-All” yöntemi ile ayrı ayrı tespit sağlanmıştır. Önerilen sistemin doğruluk, yanlış alarm oranı, Alıcı Çalışma Karakteristiği (Receiver Operating Characteristic-ROC) ve Hassas-Geri Çağırma Eğrileri (Precision-Recall Curves-PRC) açısından çok daha iyi performans gösterdiğini sunmuşlardır [64].

Zoghi ve diğ. (2021) çalışmalarında UNSW-NB15 veri setini kullanmadan önce ele alınması gereken sınıf dengesizliği ve sınıf çakışması problemlerini ele almışlardır. Görsel analize hazırlık olarak, gereksiz özelliklerin kaldırılması, özelliklerin normalleştirilmesini ve özelliklerin ölçeklenmesini içeren ön işleme adımları uygulamışlardır. Veri ön işleminin ardından, bu veri kümesiyle sınıf dengesizliği ve sınıf çakışması sorunlarını ortaya çıkarmak ve göstermek için çeşitli görselleştirme teknikleri kullanarak veri seti, Temel Bileşenler Analizi (Principal Component Analysis-PCA) kullanılarak 2B ve 3B görünümlere yansıtılmıştır. Daha sonra dağılım grafiği, t-SNE ve K-ortalama kümeler arası mesafe haritası ile analiz edilmiştir. Herhangi bir veriye dayalı istatistiksel veya ML modelinin sınıflandırma performansı üzerindeki olumsuz etkilerini azaltmak için etkili yaklaşımların uygulanmasının zorunlu olduğunu savunmuşlardır [65].

Aleesa ve diğ. (2021) çalışmalarında UNSW-NB15 veri setinin modellerinin her dosya için ayrı ayrı test edilmesi yerine, tüm veri setini tek bir dosyada birleştirerek modellerin bir kez test edebilmesini amaçlamışlardır. Daha sonra veri kümesindeki saldırı türlerini yeni bir sınıf olarak kullanmış, böylece çoklu sınıflandırma etiketli veri kümesi geliştirmeyi hedeflemişlerdir. Geliştirdikleri veri seti ile derin öğrenmenin performansını İkili ve Çoklu Sınıf (Binary ve Multi-Class) olarak iki sınıflandırma kategorisi içinde araştırmışlardır. Önerilen derin öğrenme modellerinin, çok sınıflı sınıflandırmada %99,59 ve ikili sınıflandırmada %99,26 doğruluk sağladığını tespit etmişlerdir [66].

Kocher ve diğ. (2021) UNSW-NB15 veri setini KNN, Stokastik Gradyan Azalma (Stokastik Gradient Descent-SGD), RF, LR ve NB gibi sınıflandırıcıları eğitim için kullanılmışlardır. Filtre tabanlı bir öznetelik seçme tekniği olan Ki-Kare, alakasız ve gereksiz özellikleri azaltmak için UNSW-NB15 veri kümesine uygulanmış; sınıflandırıcıların performansı, doğruluk, Ortalama Kare Hata (Mean Squared Error-MSE), kesinlik, geri çağırma,

F1-Skoru, Gerçek Pozitif Oranı (True Positive Rate-TPR) ve Yanlış Pozitif Oranı (False Positive Rate-FPR) ile öznitelik seçme tekniği ile karşılaştırmalı analiz yapılmıştır [67].

Mahalakshmi ve diğ. (2021) UNSW-NB15 veri seti üzerinde Evrişimli Sinir Ağları (Convolutional Neural Network-CNN) derin öğrenme yöntemini kullanarak binary şeklinde kodlanan veri setinin maksimum başarımlarını gösterdiğini kanıtlamışlardır [68].

Iqbal ve diğ. (2021) çalışmalarında, PyCaret makine öğrenimi kitaplığını kullanarak ve genel performansını analiz ederek IoT ağlarındaki botnetleri tespit etmek için daha verimli bir makine öğrenimi yaklaşımı amaçlanmıştır [69].

Sharma ve diğ. (2021) çalışmalarında, RF, XT, AdaBoost, XGBoost yöntemlerini kullanarak veri seti üzerinde bir takım işlemler uygulayarak makine öğrenmesi metodları ile saldırı tespitinin doğru olup olmadığı değerlendirmişlerdir [70].

Sarhan ve diğ. (2022) çalışmalarında, UNSW-NB15, BoT-IoT, ToN-IoT, CSE-CICIDS2018 veri seti üzerinden önerilen NetFlow tabanlı özellik setleriyle yeni varyantlara dönüştürmüş; XT sınıflandırıcısını temel alarak, NetFlow tabanlı özellik kümelerinin sınıflandırma performansını orijinal veri kümeleriyle sağlanan tescilli özellik kümeleriyle karşılaştırmışlardır [71].

Pacheco ve diğ. (2021) çalışmalarında UNSW-NB15 ve Bot-IoT veri kümelerinin Multi-Layer Perceptron (Çok Katmanlı Algılayıcı-MLP), DT, RF ve SVM gibi popüler derin öğrenme saldırı yöntemlerine karşı güvenlik açığını ve çeşitli makine öğrenimi sınıflandırıcılarının güvenilirliği değerlendirmişlerdir [72].

Kılınçer ve diğ. (2021) yapmış olduğu çalışmada, STS'lerin geliştirilmesinde yaygın olarak kullanılan CSE-CIC IDS-2018, UNSW-NB15, ISCX-2012, NSL-KDD ve CIDDS-001 veri setlerinin kullanıldığı literatür çalışmaları detaylı olarak incelemişlerdir. Ayrıca bu veri setleri üzerinde max-min normalizasyonu gerçekleştirilmiş ve klasik makine öğrenmesi yaklaşımlarından SVM, KNN, DT algoritmaları ile sınıflandırma yapmışlardır [73].

Kushwah ve diğ. (2021) çalışmalarında Kendinden Uyarlamalı Evrimsel Aşırı Öğrenme Makinesi'ne (Self-Adaptive Evolutionary Extreme Learning Machine-SaE-ELM) dayalı bir DDoS saldırı tespit sistemi sunmuşlardır [74].

Roy ve diğ. (2021) çalışmalarında, SVM ve NB algoritmasını kullanan bir teknik önermiş, bunu kullanarak saldırı tespit sisteminin sınıflandırma problemini çözeceklerini iddia etmişlerdir [75].

Ahsan ve diğ. (2021) çalışmalarında, CNN, LSTM, Çift Yönlü (Bidirectional) LSTM (Bi-LSTM), Geçitli Tekrarlayan Birimler (Gated Recurrent Units-GRU) ve RF yöntemlerini

kullanmış doğruluk oranları çıkarmış ve daha sonra önermiş oldukları algoritma ile önemsiz değişkenler filtreleyerek, özellikleri düşürmüş ve daha doğru tahmin olanağı sağlamışlardır [76].

Pooja ve diğ. (2021) çalışmalarında, derin öğrenme yöntemine ve Bi-LSTM'ye dayalı bir kimlik modeli uygulamışlardır. Tasarlanan sistemin test edilmesi için deneylerde KDDCUP-99 ve UNSW-NB15 veri setleri kullanılmıştır. Bi-LSTM kullanan model, hem KDDCUP-99 hem de UNSW-NB15 veri kümeleri için %99 doğrulukla sonuçlar vermiştir. Ayrıca ağda kullanılan aktivasyon fonksiyonları değiştirilerek çalışma tekrarlanmıştır [77].

Thirimanne ve diğ. (2021) çalışmasında, NSL-KDD ve UNSW-NB15 veri kümeleri kullanılarak eğitilmiş saldırı tespiti için en iyi makine öğrenimi algoritmasını tespit etmek ve denetimli, yarı denetimli ve denetimsiz öğrenme olarak sınıflandırılan altı makine öğrenimi algoritması arasında karşılaştırmalı bir analiz yapmayı amaçlamışlardır. Çalışmada, denetimli ve yarı denetimli makine öğrenimi algoritmalarının performansının, her iki veri kümesi için denetimsiz makine öğrenimi algoritmalarından daha iyi performans gösterdiği ortaya konulmuş, SVM ve DNN sırasıyla NSL-KDD ve UNSW-NB15 için daha iyi performans gösterdiği görülmüştür [78].

Rani ve diğ. (2022) çalışmalarında, sınıf dengesizliği çözümüne yönelik derin sinir ağı önermişlerdir. Ağ verileri, veri dönüştürme ve ardından min-maks normalleştirme yöntemiyle ön işleme tabi tutulmuş Yapay Sinir Ağları (Neural Networks-NN) yöntemiyle analiz gerçekleştirilmiştir [79].

Okay ve diğ. (2021) çalışmalarında, WLAN'lar için mevcut STS'lerdeki eksiklikleri azaltmak ve bilinmeyen ve karmaşık saldırı varyantlarını dinamik olarak tespit edebilen daha etkili bir sistem oluşturmak amaçlanarak, bu bağlamda bir metodoloji önerilmiştir. Önerilen metodolojinin temel olarak iki önemli katkısı iddia edilmiştir. İlk katkının, kullanılan özelliklerin sayısını azaltarak saldırı tespit hızını artıran Özellik Seçimi Yaklaşımı (Feature Selection Approach-FSAP) kullanılması olduğu, ikinci katkının, saldırıları hızlı ve yüksek doğrulukla tespit eden İmza ve Anomali Tabanlı Saldırı Tespit Tekniği (Signature and Anomaly Based Attack Detection Technique-SABADT) ile hibrit saldırı tespit yaklaşımı olduğu savunulmuştur. Önerilen metodoloji, KDD'99 ve UNSW-NB15 veri setlerinde uygulanmıştır. Elde edilen sonuçlar mevcut makine öğrenme teknikleri ile karşılaştırılmıştır. Tespit modeli, KDD'99 ve UNSW-NB15 eğitim veri setleri kullanılarak oluşturulmuş ve KDD'99 ve UNSW-NB15 test veri setleri üzerinde test edilmiştir. Elde edilen %99.65 ve %99.17 doğruluk oranları literatürdeki öncü yöntemler ile kıyaslandığında oldukça yüksek olarak değerlendirilmiştir.

Ayrıca, çalışma kapsamında yeni saldırıları test etmek için normal aktiviteler ve mevcut saldırı davranışlarının bir karışımını elde etmek için ortak araçlar kullanılmıştır. Wireshark aracıyla farklı saldırı türleri yakalanmış, yakalanan saldırıların bazıları yalnızca test aşamasında kullanılmıştır. Bu test durumunda ise saldırılar %99,69 doğruluk oranıyla tespit edilmiştir [80].

Sekhar ve diğ. (2021) çalışmalarında, “Fruitfy Optimizasyonu ile Deep Autoencoder kullanan yeni bir Saldırı Tespiti Tekniği” önermişlerdir. İlk olarak, veri kümesindeki eksik değerler, önemli bilgileri korurken bulanık ve kaba kümelerden yararlanarak veri kümelerindeki belirsizliği işleyen Fuzzy C-Means Rough Parameter (FCMRP) algoritması ile değiştirilmiştir. Ardından, çoklu gizli katmanlarla Autoencoder'dan sağlam özellikler çıkarılmıştır. Son olarak, elde edilen öznitelikler, saldırıları sınıflandırmak için Geri Yayımlı Sinir Ağı (Backpropagation Neural Network-BPN) ile beslenmiştir. Ayrıca Deep Autoencoder'ın gizli katmanlarındaki nöronlar, popülasyon tabanlı Fruitfy Optimization algoritması ile optimize edilmiştir. NSL\_KDD ve UNSW-NB15 veri seti üzerinde deneyler yapılmıştır. BPN'li derin otomatik kodlayıcı kullanarak önerilen saldırı tespit sisteminin hesaplama sonuçları, NB, SVM, Radyal Temel İşlev Ağı (Radial Basis Function Networks-RBFN), BPN ve Softmax'lı Otomatik Kodlayıcı ile karşılaştırılmıştır [81].

İnternetin hızlı gelişimi ile siber saldırı yöntemleri daha karmaşıklaşmış ve dünyaya verdiği zarar giderek daha büyük hale gelmiştir. Bu nedenle, Yang (2021)'ın internetteki kötü niyetli davranışların zamanında tespiti, günümüzde önemli bir güvenlik sorunu haline geldiğinden yola çıkarak gerçekleştirdiği çalışmada, derin öğrenmeye dayalı bir STS önermekte, sisteme çift yönlü LSTM mimarisini uygulamakta ve eğitim ve test için UNSW-NB15 veri setini kullanmaktadır. Çalışmadaki deneysel testler, STS'nin mevcut ağ ortamında ağın bilinen veya bilinmeyen kötü niyetli davranışlarını etkili bir şekilde tespit edebildiğini göstermiştir [82].

Han ve diğ. (2022) çalışmalarında, DNN özellik çıkarıcısını ve Yakınsal Politika Optimizasyonuna (Proximal Policy Optimization-PPO) dayalı bir pekiştirici öğrenme modeli olarak k-ortalama kümeleme modülünü kontrol eden ve eğiten bir Saldırı Tespit Hiperparametre Kontrol Sistemi (Intrusion Detection Hyperparameter Control System-IDHCS) önermektedir. IDHCS, ağ ortamındaki en değerli özellikleri çıkarmak için DNN özellik çıkarıcı kullanılmış ve k-arac kümeleme yoluyla izinsiz girişleri tanımlamıştır. PPO tabanlı pekiştirmeli öğrenme modelini ve yinelemeli öğrenme kullanan sistem, IDHCS'nin kullanıldığı ağ ortamına göre performansı otomatik olarak iyileştirecek şekilde optimize edilmiştir. Çalışmada, CICIDS2017 ve UNSW-NB15 veri setleri kullanılarak sistem performansını değerlendirmek

için deneyler yapılmıştır. CICIDS2017'de 0,96552'lik bir F1 puanı elde edilmiş ve UNSW-NB15, 0,94268'lik bir F1 puanına ulaşılmıştır. Daha kapsamlı ve karmaşık bir test ortamı oluşturmak için iki veri kümesi birleştirilerek bir takım deneyler yapılmıştır. Veri kümelerini birleştirerek, deneydeki saldırı türleri daha çeşitli hale getirilmiştir. Birleştirilmiş veri setinde 0,93567 F1 puanı elde edilmiş, CICIDS2017 ve UNSW-NB15 ile karşılaştırıldığında %97 ila %99 performans elde edilmiştir. Ulaşılan sonuçlar, önerilen IDHCS'nin, sürekli öğrenme yoluyla ağ ortamındaki değişikliklerden bağımsız olarak izinsiz giriş tespit özelliklerini kullanıp yeni saldırı türlerini tespit etmeyi otomatikleştirerek STS'nin performansını iyileştirdiğini ortaya koymuştur [83].

Al-Gethami ve diğ. (2021) çalışmalarında, DT, RF, SVM, ANN ve NB kullanılarak ML tabanlı STS'lerin sınıflandırma doğruluğunun belirli faktörlerden etkilenebileceğini göstermek amaçlanmıştır. Çalışmada ele alınan faktörler, eğitim ve test için veri setini kullanma yöntemi, aykırı değerlerin ve uç değer örneklerinin kaldırılması, yanlış etiketlenmiş örneklerin eklenmesi ve topluluk öğrenme tekniklerinin kullanılmasıdır. Bu faktörlerin sınıflandırma doğruluğu üzerinde çeşitli etkileri gösterilmiş; bazı durumlarda, verilerde oluşan gürültünün RF algoritmasının doğruluğu üzerindeki etkisi, sınıflandırma doğruluğu üzerinde olumsuz etkileri gösterilmiştir. Bu faktörlerin olumsuz etkilerinin, UNSW-NB15 veri kümesine uygulandığında DT, RF, SVM, ANN ve NB algoritması gibi sınıflandırma yöntemleriyle büyük bir iyileşme sağladığı gösterilmiştir [84].

Meliboev ve diğ. (2022) çalışmalarında, CNN, LSTM, Yinelemeli Sinir Ağı (Recurrent Neural Network-RNN) ve Geçitli Tekrarlayan Birimler (Gated Recurrent Unit-GRU) yöntemleri kullanılarak etkili ve uyarlanabilir STS uygulamak için bir DL yöntemi önermişlerdir [85].

El-Sayed ve diğ. (2021) çalışmalarında, akıllı taşıma sistemlerinde saldırı tespitine yönelik bir öneri sunulmuştur. Bu öneri için veri setindeki yalnızca 20 özellik kullanılmıştır. Yöntem olarak SVM, ANN ve NB algoritmaları kullanılmış, önerilen yöntem ile doğruluk değerinin arttığı tespit edilmiştir [86].

Kim ve diğ. (2021) çalışmalarında, UNSW-NB15 veri seti ile dört tip STS saldırısını tahmin etmek için makine öğrenme tekniklerinden LSTM kullanarak tahmin alanındaki saldırıların zamanlamasını tahmin eden bir model önermişlerdir. Her saldırı için, örneklerin %80'i ve %90'ı LSTM girdileri olarak kullanılmış ve bu modeli eğitirken epoch değerlerini 1'den 26'ya yükseltmişlerdir. Bu model Arka Kapı (Back Door), DoS, Zayıflık (Exploit) ve Generic saldırıları için saldırı noktalarını tahmin etmiştir. Model tarafından üretilen çıktı

değerleri, saldırının tam zamanlamasını doğrulamak için analiz edilmiştir. Dos, Backdoor ve Generic'te,  $T[i]$ 'nin gerçek saldırı zamanlamasına karşı  $T[i]+2$  zaman diliminde saldırı noktası beklediklerini bulmuşlardır. Bununla birlikte, bir Exploit saldırısı durumunda, ardışık örtüşen saldırıların meydana geldiğini, LSTM tarafından hesaplanan sayısal değerlerin yorumlanmasında belirsizlik olduğunu ve bunun da bir saldırının olup olmadığını belirlemeyi zorlaştırdığını belirtmişlerdir [87].

Hossain ve diğ. (2021) çalışmalarında, DT, SVM, RF ve NB olmak üzere dört popüler sınıflandırıcının, Pandas ve SKlearn kitaplıkları ile birlikte Python dilini kullanarak UNSW-NB15 veri kümesi üzerindeki performansını değerlendirmişlerdir. 43 özelliğe sahip UNSW-NB15 veri setini eksiksiz bir şekilde kullanmışlardır. Gerçekleştirilen deneysel sonuçlar, RF, DT ve NB için doğrulukta Apache Spark ve onun MLlib'i tarafından üretilen daha önce bildirilen sonuçlara göre iyileşme olduğunu göstermiştir [88].

Dutt ve diğ. (2021) iğherleri çalışmalarında, saldırı tespitinde yaygın olarak kullanılan iki veri kümesi olan KDD'99 ve UNSW-NB 15 veri setlerini detaylı bir şekilde ele almış ve analiz etmişlerdir. Weka veri madenciliği aracı kullanılarak veri temizleme işlemi ile birlikte eksik, fazlalık ve gürültülü veriler dikkate alınarak her iki veri setinin ön işlemei gerçekleştirilmiştir. Ek olarak bir haftalık ağ trafiği kullanılarak yeni bir veri seti sunulmuştur. Bu veri seti, bu tür özelliklerin izinsiz girişleri belirlemede önemli bir rol oynadığı tespit edildiğinden kaynak tüketimine dayalı özellikler dikkate alınarak hazırlanmıştır. Ayrıca, izinsiz giriş tespit sistemlerine de uygulanabilen herhangi bir tahmin durumunda ön işlemenin çok önemli bir rol oynadığına dikkat çekilmiştir. KDD'99 ve UNSW-NB15 veri setlerinin ön işlemei Weka veri madenci aracı kullanılarak gösterilmiştir [89].

Kim ve diğ. (2021) çalışmalarında, bir STS veri kümesi olan UNSW-NB15'e LSTM ve GRU uygulayarak saldırıların zamanlamasını tahmin etmek için bir derin öğrenme modeli önermişlerdir. Model doğruluğunu artırmak için kayan nokta değerlerini eşdeğer ikili değerlere dönüştürmek için sonlu durum makinesi konseptini uygulamışlardır. Sonuç olarak ağırlıklı F1 puanı açısından GRU ve LSTM'nin doğruluğu sırasıyla ortalama %13 ve %18 olarak bulmuşlardır [90].

Saldırı tespit sistemleri, ICT altyapısını (STS'ler) korumak için kritik bileşenlerdir. Farklı yeni saldırı türleri ve karmaşıklık kontrolü için sağlam bir çözüm sağlamak adına derin öğrenme ve makine öğrenimi, yüksek boyutlu, karmaşık türdeki verileri işlemek için yaygın olarak kullanılan çözümlerdendir. STS, denetimsiz makine öğrenimi tekniklerini kullanarak bilinen, bilinmeyen ve sıfırcı gün saldırıları gibi çeşitli saldırı türlerini algılamakta ve

çekmektedir. Sing ve diğ. (2021) çalışmalarında, tehditleri önceden bilgi kaybı olmadan tespit etmek için, Tek Sınıf SVM (OCSVM) kavramını ve aktif öğrenmeyi kullanan bir yapı tasarlamışlardır. Gerçekleştirilen çalışmanın performansını test etmek ve sonucu UNSW-NB15 ve KDD cup 99 veri seti ile karşılaştırmak için ise CIC-IDS2017 veri seti kullanılmıştır. Geliştirilen bu yapının daha iyi performans gösterdiği kanıtlanmıştır [91].

Silva ve diğ. (2022) çalışmalarında, ağ üzerinde gerçekleşen izinsiz giriş tespit etmek için makine öğrenimi mekanizmaları kullanma aşamasında, iyi yapılandırılmış veri kümelerinin azlığı nedeniyle doğru değerlendirme, karşılaştırma ve dağıtımdan yoksun olduğuna dikkat çekmişlerdir. Bu sıkıntıdan yola çıkılarak en çok kullanılan dört veri setinde yer alan özelliklerin istatistiksel bir analizini önermişlerdir. Analiz edilen veri kümelerinin izinsiz giriş tespit sistemleri için yeni anormallik tabanlı mekanizmalar oluşturmak için bir kıyaslama olarak kullanılmaması gerektiği sonucuna varılmış olup önerilen metodoloji ile, fazla değerleri veya veri dengesizliğini kontrol etmek yerine özellikler arasındaki korelasyonu analiz etmişlerdir. Analiz aşamasında DT, LR, RF ve XGBoost yöntemlerini uygulamışlardır [92].

Priya ve diğ. (2021) çalışmalarında, KDDCUP99, DARPA 1999, TWENTE 2008, UNIBS 2009, ISCX2012, NGIDS-DS 2016, UNSWNB15, CICIDS2017 veri setleri ile Sigmoid sınıflandırıcı karşılaştırılarak, STS veri setlerinin performans analizi ve öznelite analizini birlikte sunmuşlardır [93].

Man ve diğ. (2021) çalışmada, öğrenmeye dayalı bir ağ saldırı tespit modeli önermişlerdir. Çalışmada öncelikle, veri setini bir ön işleme tuttuktan sonra veri setini görüntülere dönüştürmüşlerdir. Daha kritik özellikleri öğrenmek için artık bloklara sahip daha derin evrişimli sinir ağları oluşturulmuş, çapraz entropi işlevi yerine, eğitim setindeki sınıf dengesizliği sorununu ele almak ve test setindeki küçük saldırıları belirlemek için odak kaybı hesaplanmıştır. Modelin yanlış tespitlerini önlemek ve geliştirmek için toplu normalleştirme ve küresel ortalama havuzlama yöntemleri kullanılmıştır. Gerçekleştirilen işlemler sonucunda, önerilen modelin mevcut modellere kıyasla saldırı tespit doğruluğunu iyileştirebileceğini gösterilmiştir [94].

Ashiku ve diğ. (2021) çalışmalarında, ağ saldırılarını tespit etmek ve sınıflandırmak için uyarlanabilir ve esnek bir ağ STS geliştirmek için derin öğrenme mimarilerinin kullanımını önermektedir. Çalışmada, yaygın siber güvenlik açıklarını içeren ağ trafiği veri setini kullanan ağ saldırı tespit sistemleri ele alınmış; yarı dinamik hiper parametre ayarlama yaklaşımıyla birleştirilmiş bu sistem, derin öğrenme sınıflandırma mimarisi, benzer derin öğrenme tabanlı ağ STS'lerinin sonuçlarına kıyasla çok sınıflı modellerde önemli gelişmeler göstermiştir.

Önerilen yaklaşımın, önceden bölümlenmiş ve kullanıcı tanımlı çok sınıflı sınıflandırma için %95,4 ve %95,6 genel doğruluk elde ettiğini göstermiştir [95].

Hooshmand ve diğ. (2022) çalışmalarında, tek boyutlu CNN mimarisini kullanan bir model önermektedir. Önerilen yaklaşım, ağ trafik verilerini ilk aşamada İletim Kontrol Protokolü (Transmission Control Protocol-TCP), Kullanıcı Datagram Protokolü (User Datagram Protocol-UDP) ve diğer protokol kategorilerine ayırmaktadır. Daha sonra her kategori bağımsız olarak ele alınmıştır. Modeli eğitmeden önce, Ki-kare tekniği kullanılarak öznitelik seçimi gerçekleştirilmiş ve ardından bir sınıf dengesizliği problemini çözmek için sentetik azınlık aşırı örnekleme tekniği kullanılarak aşırı örnekleme yapılmıştır. Önerilen yöntem sırasıyla TCP, UDP, OTHER ve ALL kategorileri için ağırlıklı ortalama f-skoru 0.85, 0.97, 0.86 ve 0.78 vermiştir [96].

Kamarudin ve diğ. (2021) çalışmasında, veri setindeki en önemli özellikleri belirlemek ve anormal ağ etkinliklerini daha doğru bir şekilde analiz etmek adına ML ile DoS saldırılarının tespitindeki doğruluğu geliştirmeyi amaçlanmaktadır. RF yöntemi kullanarak önerilen sistemin doğruluk oranı deneysel sonuçlarla gösterilmiştir. Her bir veri setindeki doğruluk oranının geleneksel yaklaşımlarla karşılaştırıldığında yüzde 98,8'den fazla olduğu tespit edilmiştir [97].

Magan-Carri'on ve diğ. (2021) tarafından gerçekleştirilen çalışmada, ML tabanlı Ağ STS için yeni bir metodoloji olan Reliable-NIDS (R-NIDS) adını verdikleri bir yöntem sunmuşlardır. Ayrıca UNK21 adında yeni bir veri seti önermişlerdir. Sistemi en iyi bilinen üç saldırı veri setinden (UGR'16, USNW-NB15 ve NLS-KDD) toplayarak, her biri kendi ağ ortamından, farklı özellikler ve sınıflarla, mevcut bir veri toplama yaklaşımı kullanılarak oluşturmuşlardır. Bu veri seti ile saldırı tespit oranındaki doğruluk değerinin arttığını göstermişlerdir [98].

Sharma ve diğ. (2021) çalışmalarında, RF, XT, AdaBoost ve XGBoost yöntemlerini kullanarak UNSW-NB15 veri seti üzerinde saldırı tespit doğruluk oranını arttırmak amaçlanmıştır. Kullanılan tüm sınıflandırıcılar arasında karşılaştırmalı bir analiz için tüm standart değerlendirme parametreleri hesaplanmış; her bir özellikteki aykırı değerleri incelemek için grafiklerden faydalanmışlardır. Elde edilen grafikler her sınıf etiketi için her özelliğin minimum, maksimum ve medyan değeri hakkında fikir vermiştir. Verilerin grafik analizleri ile birlikte her bir özelliğin frekans dağılımı sunulmuş; özellikler arasındaki korelasyon açıklanmıştır. Nokta çizimleri, saldırı etiketleri için her bir özelliğin ortalama değerinin sıfır civarında olduğunu ve normal sınıf etiketleri için büyük ölçüde değiştiğini gözlemlemişlerdir. Rastgele orman sınıflandırıcısının %86,9 doğrulukla en iyisi olduğu tespit edilmiş ve tüm

sınıflandırıcıların performanslarının çok az değişmesine ve neredeyse benzer sonuçlar vermesine rağmen, AdaBoost yönteminin en düşük doğruluğu elde ettiği görülmüştür [99].

Chew ve diğ. (2021) tarafından gerçekleştirilen çalışmada, seçilen üç NIDS veri setini değerlendirmek için 10 önemli makine sınıflandırıcısı (ZeroR, Random Tree, REPTree, Decision Stump Adaboost, Bayesnet, NB, RF, SMO ve J48) kullanılmıştır. Gerçekleştirilen analizlerle UNSWNB15 veri setinin düşük ayak izi senaryosunda saldırı tespiti için daha uygun olduğu, CIDDs-001 veri setinin keşif tekniklerini tespit etmek için uygun olduğu, GureKDDCup ise önceki kıyaslama KDDCup'99'a benzer özelliklerin çoğunu içerdiği ve önceki kıyaslama yerine kullanılabilir veri kümesi olduğu belirlenmiştir [100].

Acharya ve diğ. (2021) çalışmalarında, Weka kullanılarak KDD99, UNSW-NB15 ve CIC-IDS2017 ağ günlükleri trafiğini kullanan veri setleri üzerinde RF, J48, NB, BayesNet, Bagging, AdaBoost ve SVM dâhil olmak üzere çeşitli makine öğrenimi algoritmalarının etkinliği tartışılmıştır. Ağ saldırı veri kümelerinin çıktı sınıflarının sayısının değiştirilmesinin duyarlılık, TPR, FPR, ROC Eğrisi Altındaki Alan (Area Under Curve-AUC) ve yanlış tanımlanan yüzde üzerindeki etkisini incelemişlerdir. Hedef sınıf sayısı azaldığında makine öğrenimi sınıflandırıcılarının performansının arttığı ve çıktı sınıfına yüksek düzeyde ilişkili bir özelliğin eklenmesiyle, sınıflandırıcıların performansının arttığı ortaya konulmuştur [101].

Dlamini ve diğ. (2021) çalışmalarında, anomali tespit alanındaki doğruluk tespitini iyileştirmek için DGM adını verdikleri bir veri üretici modeli bir sistem tanıtmışlardır. Yaklaşımın etkinliğini göstermek için NSL-KDD ve UNSW-NB15 veri setleri üzerinde deneyler gerçekleştirmişlerdir. Mevcut istatistiksel yaklaşım SMOTE ile kendi yöntemlerini karşılaştırmışlar ve DGM'nin daha iyi performans göstermişlerdir [102].

Pavlov ve diğ. (2021) çalışmalarında, ağ üzerinde izinsiz giriş tespit sistemlerinde kullanım için veri kümeleri gereksinimlerinin oluşturulmasına yönelik mevcut yaklaşımlar ele alınmış ve modern veri kümeleri analiz edilmiştir. Saldırgan gruplarını tanımlamaya yönelik test yöntemlerinde kullanımları için veri kümeleri için bir gereksinim listesi oluşturulmuştur. Gereksinimler için ağırlıklar belirlenmiş ve modern veri kümeleri için bir kullanılabilirlik derecesi belirlenmiştir. Ayrıca mevcut veri kümeleri tarafından yetersiz şekilde ele alınan gereksinimleri karşılamak için alternatif bir veri kaynağı önerilmiştir [103].

Güler ve diğ. (2021) çalışmalarında, UNSW-NB15 veri seti üzerinde ağlarda saldırı tespiti için denetimli öğrenme sınıflandırması tabanlı RNN, LSTM ve GRU algoritmaları karşılaştırmalı olarak uygulamışlardır. Çalışmanın temel amacı, derin öğrenme algoritmalarının başarısını karşılaştırmak ve saldırı tespiti ve sınıflandırması için en uygun modele ulaşmaktır.

Modellerin doğruluk değerleri %98 ve FPR değerleri RNN, LSTM ve GRU modelleri için sırasıyla 0.014, 0.011 ve 0.011 olarak bulunmuştur [104].

Tablo 2.13'te veri seti ile ilgili yapılan çalışmaların karşılaştırılmasına yer verilmiştir. Tablonun incelenmesiyle literatüre genel bir bakış sağlanacağı değerlendirilmektedir. "Tartışma" bölümünde bu tabloda verilen kaynaklardan gerçekleştirilen sistem ile en uygun olanların karşılaştırması ve tartışmasına yer verilecektir.

**Tablo 2.14:** Veri seti ile ilgili yapılan çalışmaların karşılaştırılması

| K.N  | TESPİT EDİLEN SALDIRI/ ODAKLANILAN KONU                                                                                                                                | KULLANILAN YÖNTEM                                                                                                          | YIL  | VERİ SETİ                                      | GELİŞTİRME ORTAMI                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------|----------------------------------------------------------|
| [64] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | SMOTE Yöntemi, Extremely Randomized Trees Sınıflandırıcı, Extreme Learning Machines (ELM) Modeli                           | 2021 | UNSW-NB15                                      | Python                                                   |
| [65] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | t-SNE ve K-ortalama kümeler arası mesafe haritası                                                                          | 2021 | UNSW-NB15                                      | Python                                                   |
| [66] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | Deep Neural Network (DNN), Artificial Neural Network (ANN), Long Short-Term Memory (LSTM)                                  | 2021 | UNSW-NB15                                      | Matlab                                                   |
| [67] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | K-En Yakın Komşular (KNN), Stokastik Gradient Descent (SGD), Random Forest (RF), Lojistik Regresyon (LR), Naive Bayes (NB) | 2021 | UNSW-NB15                                      | Python                                                   |
| [68] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | Convolutional Neural Network (CNN)                                                                                         | 2021 | UNSW-NB15                                      | Python                                                   |
| [69] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | KNN, RF, LR, NB, DT, Gradient Boosting Classifier, Adaptive Boot Classifier, Blending.                                     | 2021 | UNSW-NB15                                      | Google Colaboratory-PyCaret Library                      |
| [74] | DDoS                                                                                                                                                                   | SaE-ELM-Ca Model                                                                                                           | 2021 | NSL-KDD, ISCX IDS 2012, UNSW-NB15, CICIDS 2017 | Matlab                                                   |
| [76] | Accuracy, Precision, F1-score, AUC                                                                                                                                     | CNN, LSTM, RF, Bidirectional LSTM (Bi-LSTM), Gated Recurrent Units                                                         | 2021 | NSLKDD, UNSW-NB15                              | Anova                                                    |
| [77] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode, Probing Attack, User-to-Root attack (U2R), Remote-to-local Attack (R2L) | Bi-LSTM                                                                                                                    | 2021 | KDDCUP-99, UNSW-NB15                           | Python (keras, numpy, sci-kit learn, pandas, matplotlib) |
| [78] | Precision, Recall, F1-score, ROC                                                                                                                                       | DNN, K-NN, SVM, OCSVM, K-Means, EM                                                                                         | 2022 | NSLKDD, UNSW-NB15                              | Python                                                   |
| [79] | Precision, Recall, F1-score, ROC                                                                                                                                       | Neural Networks (NN)                                                                                                       | 2022 | NSLKDD, UNSW-NB15                              | Python, Apache Spark                                     |
| [80] | Denial of Service (DoS), User-to-Root (U2R), Remote-to-Locals (R2L), Probe                                                                                             | NB, SVM, RBFN, Conventional BPN                                                                                            | 2021 | NSL_KDD, UNSW-NB15                             | Python                                                   |
| [82] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | Bi-LSTM                                                                                                                    | 2022 | UNSW-NB15                                      | Python (Tensorflow1.3, Keras2.1)                         |
| [84] | Accuracy, Precision, Recall                                                                                                                                            | DT, RF, SVM, NB, ANN                                                                                                       | 2021 | KDD'99, UNSW-NB15                              | Weka                                                     |
| [85] | Accuracy, Precision, Recall, F-Score                                                                                                                                   | CNN, LSTM, RNN, GRU                                                                                                        | 2022 | UNSW NB15, KDDCup'99, NSL-KDD                  | Python                                                   |

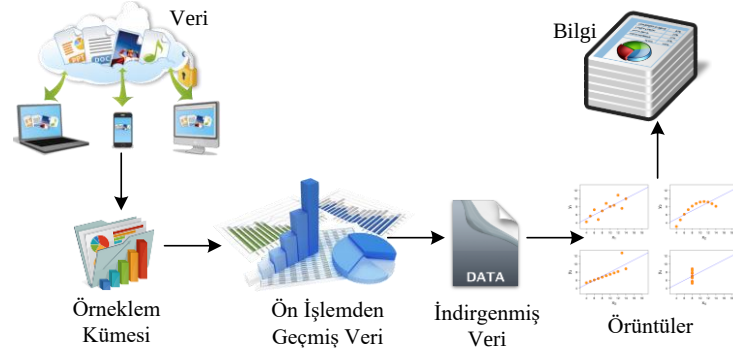
|       |                                                                                                                                                                        |                                                       |      |                                                |                                       |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|------|------------------------------------------------|---------------------------------------|
| [86]  | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | SVM, NB, DNN                                          | 2021 | UNSW NB15                                      | Google Colab                          |
| [87]  | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | LSTM                                                  | 2021 | UNSW NB15                                      | Keras                                 |
| [88]  | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | DT, SVM, RF, NB                                       | 2021 | UNSW NB15                                      | Apache Spark (Mllib, Pandas, Sklearn) |
| [90]  | Backdoor, DoS, Generic, Exploits                                                                                                                                       | LSTM, GRU                                             | 2021 | UNSW-NB15                                      | Python, Pycharm                       |
| [91]  | Total, Normal, Dos, Probe, R2L, U2L                                                                                                                                    | Tek Simf SVM (OCSVM)                                  | 2021 | UNSW-NB15, KDD cup 99, CIC-IDS2017             | Python                                |
| [92]  | Accuracy, Precision, F1-score, Recall                                                                                                                                  | DT, LR, RF, XGBoost                                   | 2022 | KDD'99, CICIDS 2017, UNSW-NB15, CICBotnet 2014 | Python                                |
| [94]  | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | CNN                                                   | 2021 | UNSW NB15                                      | Python                                |
| [95]  | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | DNN                                                   | 2021 | UNSW NB15                                      | Google Colab (Keras, TensorFlow)      |
| [96]  | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | CNN                                                   | 2022 | UNSW NB15                                      | Python 3.6 (scikit learn ve Keras)    |
| [97]  | DoS                                                                                                                                                                    | KNN, J48, RF, NB                                      | 2021 | UNSW NB15                                      | Python                                |
| [98]  | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode, Probing attack, User-to-Root attack (U2R), Remote-to-local attack (R2L) | Reliable-NID (R-NIDS)                                 | 2021 | NSLKDD, UNSW-NB15, UNK21                       | -                                     |
| [101] | True Positive Rate, False Positive Rate, ROC                                                                                                                           | RF, J48, NB, SVM, Bayesian Network, Bagging, AdaBoost | 2021 | KDD99, UNSW-NB15, CIC-IDS2017                  | Weka                                  |
| [102] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode, Probing attack, User-to-Root Attack (U2R), Remote-to-local Attack (R2L) | RF, DT, NN, SVM, C4.5                                 | 2021 | NSL-KDD, UNSW-NB15                             | Python, Sklearn                       |
| [104] | Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Worms, Reconnaissance, Shellcode                                                                          | RNN, LSTM, GRU                                        | 2021 | UNSW-NB15                                      | Visual Studio                         |

### 3. YÖNTEM

Teknolojinin hızlı gelişimine paralel olarak günümüz “Bilgi Çağı”nda bilgisayar ve internet kullanımı da hızla yaygınlaşmaya başlamıştır. Bu yaygın kullanım birçok işlemin artık elektronik ortamdan gerçekleştirilmesine sebep olmuştur. Bu durum sayısal ortamda bulunan verinin her geçen gün hızlı bir şekilde büyümesini sağlamış aynı zamanda bu yayılım, verinin karmaşıklığını da beraberinde getirmiştir. Sayısal olarak toplanan bu verilerin de analiz edilmesi gerekliliğini doğurmuştur. Bu şekilde oluşan farklı veri setlerinin ve türlerinin, farklı kullanıcıların verimli bir şekilde erişebilecekleri şekilde yönetilip ve organize edilmesini sağlaması da gereklilik haline gelmiştir. Bu nedenle de veri madenciliği tekniklerinin uygulanması gerekliliği artmış, buna bağlı olarak da artan sayıda araştırmacıların bu konuya odaklanması gerçekleşmiştir.

Veri analizi, ham verileri yararlı bilgilere dönüştürmek için kullanılan bir süreç olarak ifade edilebilmektedir. Büyük veri tabanlarından gizli tahminlerle bilgileri çıkartmaya yarayan veri analizi, şirket, kurum veya kişilerin veri ambarlarındaki en önemli bilgilere odaklanmalarına yardımcı olan, gelecekteki eğilimleri ve davranışları öngören, işletmelerin faydalı kararlar almasını sağlayan büyük bir potansiyele sahip güçlü yeni bir teknolojidir. Veri analizi temelde, verileri bölümlere ayırmak, gelecekteki olayların olasılığını değerlendirmek, verimli karar ve adımları sağlamak amacıyla sofistike matematiksel algoritmaları kullanmaktadır. Veri analizi teknikleri mevcut bilgi kaynaklarının değerini artırmak için mevcut yazılım ve donanım platformlarında hızlı bir şekilde uygulanabilmekte, yeni ürün ve sistemler ile entegre edilebilmektedir. Veri analizinin temel özellikleri şu şekilde ele alınmaktadır:

- Örüntülerin otomatik olarak bulunması
- Olası sonuçların tahmin edilmesi
- Kullanılabilir bilgiler oluşturulması
- Büyük veri kümelerine ve veri tabanlarına odaklanması
- Basit sorgu ve raporlama teknikleri ile çözülemeyen soruları cevaplanabilmesi.



**Şekil 3.1:** Veri analizi işlem adımları [105]

Şekil 3.1’de veri analizi işlem adımları verilmiştir. Verilen işlem adımları arasında, veri analizinin ilk adımı ve en önemli olan kısmı analiz edilecek ve karar çıkartılacak verinin seçim işlemidir. Veri analizi işlem adımları arasında en fazla vakit harcayan adımlardan biridir. Bu işlem adımında sistemde oluşan veri iyi seçilmeli, sonuçta alınacak kararın doğruluğu açısından iyi bir şekilde analizi gerçekleştirilmelidir.

Başarılı bir veri analizi uygulaması açısından önemli olan diğer bir adım olan ön işlemede veri, daha sonra kullanılmak üzere elverişli bir duruma getirilmektedir. Bu aşamada elde edilecek başarı, sonucun başarısını yüksek oranda etkilemektedir. Doğru ve verimli bir şekilde gerçekleştirilmiş olan ön işleme aşaması sonucunda net ve kesin olarak sonuçlara varılabilecektir.

Toplanan verilerden elde edilen örneklem kümesi verilerinin belirli bir ön işlem aşamasından geçmesi sonucu faydalı ve gerçek bilgi elde etmek amacıyla gerçekleştirilen aşama verilerin indirgeme aşamasıdır. Bu aşamada, her ne kadar belirli bir ön işlemeden geçmiş olsa da sonraki işlem adımlarında kullanılacak durumda olmayan verinin indirgeme işleminin gerçekleşmesi ve daha sonraki aşamalarda kullanılabilmesi için gerekli formata çekilmesi sağlanmaktadır.

Veri analizi ve yönteminin tam olarak uygulanması amacıyla indirgenen veriye, çalışmada elde edilmek istenen amaca yönelik olarak veri madenciliği yöntemlerinin uygulanması gerekmektedir. Bu aşama ile indirgenen veriye bilinen veri analizi tekniklerinden bir ya da daha fazlası uygulanabilir. Hatta farklı veri analizi yöntemleri birleştirilerek elde edilecek bilginin daha doğru ve net olması sağlanabilir.

Elde edilen verilere veri analizi teknikleri uygulandıktan sonra elde edilen sonuçlar üzerinde yorum yapılabilir. Yapılacak yorumların doğru olup olmadığı aynı veri üzerinde uygulanan diğer veri analizi tekniklerinin sonuçlarına göre de belirlenebilir. Yani veriye uygulanan yöntemlerden hangisinin daha doğru sonuca ulaştığı belirlenmiş olmalıdır.

Uygulanan yöntemlerin sonucunda elde edilen başarının ve buna bağlı olarak yorumlanan sonucun literatürde yer alan diğer çalışmalar ile karşılaştırılması yapılarak en iyisi sonuca varıldığına emin olunur ve sonuçlar doğrulanır [105].

### 3.1. KULLANILAN YÖNTEMLER

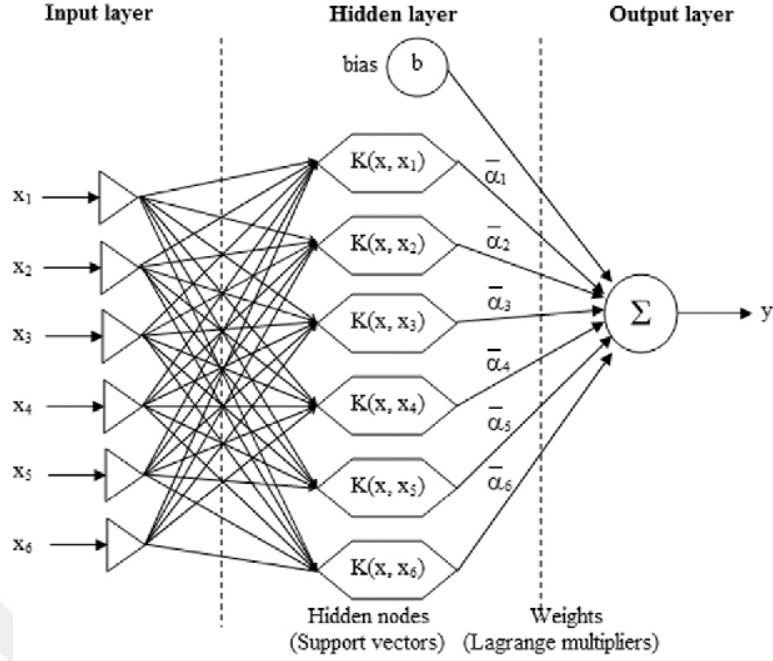
#### 3.1.1. Destek Vektör Makinesi Sınıflandırıcısı (Support Vector Machine Classifier-SVM)

SVM, hem sınıflandırma hem de regresyon için kullanılan denetimli bir makine öğrenme algoritmasıdır. SVM'nin algoritmasının temel amacı, veri noktalarını belirgin bir şekilde sınıflandıran N boyutlu bir uzayda bir hiper düzlem bulmaktır. Hiper düzlemin boyutu ise, özelliklerin sayısına bağlıdır. SVM, makine öğrenimi görevleri için ikili sınıflandırma için en yaygın ve erişilebilir yaklaşımdır.

SVM, doğrusal algoritmaları doğrusal olmayan uzaya eşlemektedir. Bu eşleme için 'çekirdek' adı verilen fonksiyon kullanılmaktadır. Doğrusal, polinom ve radyal temel işlevler gibi çekirdek işlevleri, bir hiper düzlem oluşturarak özellik uzayını bölmek için kullanılır.

Bu fonksiyonun yüzeyi boyunca destek vektörleri, çekirdek fonksiyonları kullanılarak sınıflandırıcı eğitimi sırasında tanımlanabilir. Bu yaklaşımın her örneği, iki kategoriden birine ait çeşitli eğitim örnekleriyle etiketlenmiştir. Bu aşamada, her iki veri kümesi için hangi çekirdeğin en iyi performansı gösterdiğini belirlemek için 'rbf' ve 'poly' çekirdekleri kullanılır.

C, gama ve derece gibi SVM ile ilgili hiperparametreler, grid arama yöntemi kullanılarak hiperparametre ayarlaması yapıldıktan sonra atanmıştır. SVM, yüksek boyutlu uzaylarda etkili olması, boyut sayısının numune sayısından fazla olduğu durumlarda daha etkili olması, karar işlevinde eğitim noktalarının bir alt kümesini kullanması ve bu nedenle bellek açısından da verimli olması açısından avantaj sağlamaktadır. SVM, eğer öznelilik sayısı örnek sayısından çok daha fazla ise dezavantaj sağlayacaktır. Şekil 3.2'de SVM'nin genel mimarisi sunulmuştur [111, 112].

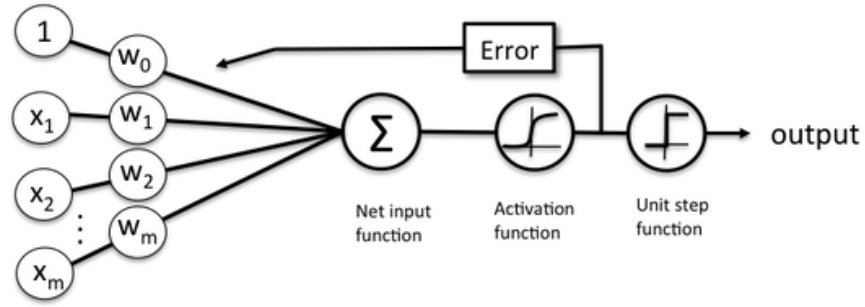


Şekil 3.2: SVM'nin genel mimarisi [111]

### 3.1.2. Lojistik Regresyon Sınıflandırıcısı (Logistic Regression Classifier-LR)

LR, verileri tanımlamak ve bir bağımlı ikili değişken ile bir veya daha fazla nominal, sıra, aralık veya oran düzeyinde bağımsız değişken arasındaki ilişkiyi açıklamak için kullanılan sınıflandırma yöntemidir.

LR, bir veri setinin önceki gözlemlerine dayalı olarak evet veya hayır gibi ikili bir sonucu tahmin etmeye yönelik istatistiksel bir yöntemdir. Bir LR modeli, bir veya daha fazla mevcut bağımsız değişken arasındaki ilişkiyi analiz ederek bir bağımlı veri değişkenini tahmin etmektedir. Birden fazla girdi kriterini işleme alabilen LR, makine öğrenimi disipliniinde önemli bir yöntem haline gelmiştir. Veriler girdi olarak yoğunlaştıkça, algoritmalar veri kümeleri içindeki sınıflandırmaları tahmin etmede daha iyi hale gelmektedir. İkili sınıflandırmanın yanı sıra, çok terimli LR, ikiden fazla olası ayrı sonucun olduğu senaryoları da modelleyebilmektedir [67, 69, 112]. Şekil 3.3'te LR'nin genel mimarisi sunulmuştur.



Şekil 3.3: LR'nin genel mimarisi [115]

### 3.1.3. Rastgele Orman Sınıflandırıcısı (Random Forest Classifier-RF)

RF, denetimli öğrenme tekniğine ait popüler bir makine öğrenme algoritmasıdır. ML'de hem sınıflandırma hem de regresyon problemleri için kullanılabilir. Karmaşık bir problemi çözmek ve modelin performansını iyileştirmek için birden fazla sınıflandırıcıyı birleştirme süreci olan topluluk öğrenme kavramına dayanmaktadır.

Bu teknikte, karar ağaçları oluşturmak için rastgele örnekler kullanılır ve ardından her ağaçtan tahmin gerçekleştirilir. RF, görüntü sınıflandırma, özellik seçimi ve öneri motorları gibi birçok uygulamaya sahiptir. Sınıflandırma için bir başka güçlü denetimli makine öğrenimi algoritması olan regresyon, bir karar ağaçları topluluğu oluşturarak çalışır. RF, birden fazla karar ağacı oluşturur ve daha doğru ve istikrarlı bir tahmin elde etmek için bunları birleştirir. Rastgele bir ormanın çoklu karar ağaçlarının bir koleksiyonu olduğu söylenebilir. Regresyon problemlerini çözmek için RF Algoritması kullanılırken 3.1'de yer alan denklem dikkate alınır: Burada  $n$ , veri noktalarının sayısıdır,  $f_i$  model tarafından döndürülen değer ve  $y_i$  i veri noktası için gerçek değerdir.

$$Rf = \frac{1}{N} \sum_{i=1}^N (f_i - y_i)^2 \quad (3.1)$$

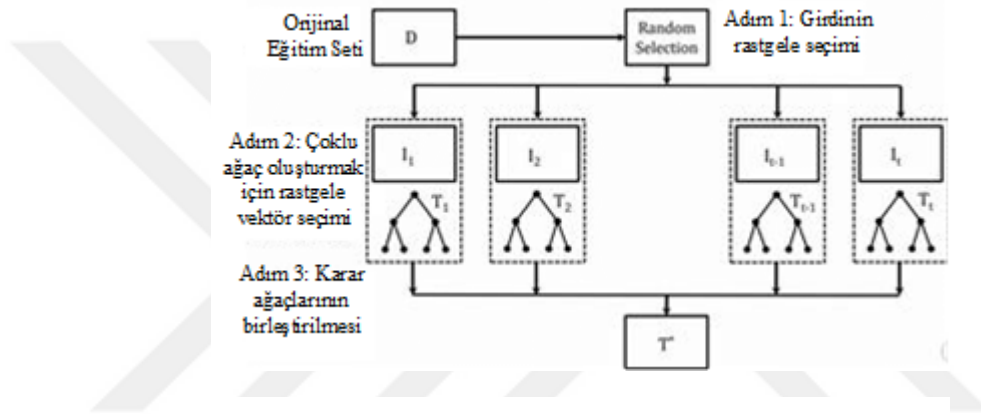
Sınıflandırma verilerine göre Rastgele Ormanlar yapılırken 3.2 numaralı denklemde görüldüğü gibi: Çoğu zaman *Gini* indeksi, sınıflandırma modelini hesaplamak için kullanılır; burada  $P_i$ , veri setinde gözlemlediğimiz sınıfın göreceli frekansını ve  $c$ , sınıf sayısını temsil eder.

$$Gini = 1 - \sum_{i=1}^c p_i^2 \quad (3.2)$$

Rastgele orman, tek bir karar ağacına güvenmek yerine, her ağaçtan ve tahminlerin çoğunluk oylarına dayalı olarak tahmini alır ve nihai çıktıyı tahmin eder. Ormandaki daha fazla ağaç sayısı, daha yüksek doğruluk sağlamakta ve uyum sorununu önlemektedir [69].

### 3.1.4. Extra Ağaçlar Sınıflandırıcısı (Extra Trees Classifier-XT)

XT, birçok karar ağacından gelen tahminleri birleştiren bir topluluk makine öğrenimi algoritmasıdır. Karar ağaçlarını oluşturmak için daha basit bir algoritma kullanmasına rağmen, genellikle RF algoritmasından daha iyi performans elde edebilmektedir. Aşırı Rastgele Ağaçlar olarak da bilinen XT, RF'den farklı olarak, orijinal veri kümesinin alt kümeleri yerine temel sınıflandırıcıları eğitmek için tüm eğitim kümesini kullanmaktadır ve rastgele seçilmektedir. Bu hiper parametreleri yapılandırmak için birkaç anahtar hiper parametresi ve mantıklı buluşsal yöntemleri olduğu için kullanımı daha kolaydır. Ağaç oluşturma sırasında karar kuralı rastgele seçilmektedir [68]. Şekil 3.4'te XT işleyiş mimarisine yer verilmiştir [112, 113].



Şekil 3.4: XT işleyiş mimarisini [112]

### 3.1.5. K- En Yakın Komşu Sınıflandırıcısı (K- Nearest Neighbour Classifier-KNN)

KNN, Denetimli Öğrenme tekniğine dayalı en basit Makine Öğrenimi algoritmalarından biridir. KNN algoritması, yeni durum/veriler ile mevcut durumlar arasındaki benzerliği ele almakta ve yeni durumu mevcut kategorilere en çok benzeyen kategoriye yerleştirmektedir. KNN, mevcut tüm verileri saklar ve benzerliğe göre yeni bir veri noktasını sınıflandırır. Bu, yeni veriler görüldüğünde, KNN algoritması kullanılarak kolayca bir kuyu paketi kategorisine sınıflandırılabilir anlamına gelir. KNN algoritması Sınıflandırmanın yanı sıra Regresyon Analizi için de kullanılmaktadır. KNN, temel veriler üzerinde herhangi bir varsayımda bulunmadığı için parametrik olmayan bir algoritma olarak değerlendirilmektedir. Tembel öğrenen algoritma olarak da adlandırılır çünkü eğitim kümesinden hemen öğrenmemekte, bunun yerine veri kümesini depolayıp sınıflandırma anında veri kümesi üzerinde bir işlem gerçekleştirmektedir. KNN, eğitim aşamasında sadece veri setini saklamaktadır ve yeni veri

aldığında bu veriyi yeni veriye çok benzeyen bir kategoride sınıflandırır [67, 69]. Şekil 3.5'te K-NN temel mantıksal yapısına yer verilmiştir.



Şekil 3.5: KNN temel mantıksal yapısı [73]

K-NN'de yeni veri noktalarının değerlerini tahmin etmek için özellik benzerliğini kullanmaktadır; bu, yeni veri noktasına eğitim kümesindeki noktalarla ne kadar yakından eşleştiğine bağlı olarak bir değer atanacağı anlamına gelmektedir. KNN'nin ilk adımında, test verilerinin yanı sıra eğitim verileri de yüklenmelidir. Daha sonra, K'nin değerini, yani en yakın veri noktaların seçilmesi gerekmektedir. Test verilerindeki her nokta için Öklid, Manhattan veya Hamming mesafesi gibi yöntemlerden herhangi birinin yardımıyla test verileri ile eğitim verilerinin her satırı arasındaki mesafeyi hesaplanır. Mesafeyi hesaplamak için en yaygın kullanılan yöntem Öklid'dir. Daha sonra, mesafe değerine göre artan düzende sıralanır. Ardından, sıralanan diziden en üstteki K satırları seçilecektir. Bu satırların en sık görülen sınıfını temel alarak test noktasına bir sınıf atayacak ve sınıflandırmayı tamamlamaktadır [73].

### 3.1.6. Karar Ağaçları Sınıflandırıcısı (Decision Tree Classifier-DT)

Sınıflandırma ve regresyon için kullanılan bir diğer popüler makine öğrenme algoritması, kararlara dayalı ağaçlar oluşturarak çalışan DT modelidir. DT yönteminde amaç, veri özelliklerinden çıkarılan basit karar kurallarını öğrenerek hedef değişkenin değerini tahmin eden bir model oluşturmaktır. Tüm veriyi kök olarak kabul ettikten sonra belirli bir koşulda, dallar veya dahili düğümler aracılığıyla bölmeye başlamaktadır ve sonucu yaprak olarak verene

kadar bir karar verme ile ilerlemektedir. Bu modeldeki *Entropi*, verilerde bulunan tarafsızlık olarak ele alınmaktadır ve 3.3'te verilen denklemle hesaplanmaktadır:

$$Entropi(S) = \sum_{i=1}^c -p(i) \log p(i) \quad (3.3)$$

Burada  $c$ , bir özneliliğin sınıf sayısıdır. ' $p(i)$ ', ' $i$ ' sınıfının örneklerinin kesridir. Örnek homojenliğe ulaştığında entropi neredeyse sıfırdır, ancak eşit olarak bölündüğünde birdir. Bu entropiyi düşürmek için "bilgi kazancı" olarak bilinen başka bir parametrenin artması gerekir. Kazancı hesaplamak için 3.4'te verilen formül kullanılır:

$$Gain(S, A) = Entropi(S) - Entropi(A) \quad (3.4)$$

3.4'te verilen formülde yer alan  $S$ , üst veya kök olarak belirlenmekte,  $A$  ise bölmek istediğimiz bir nitelik olarak ele alınmaktadır [69].

### 3.1.7. Bayes Ağları Sınıflandırıcısı (Bayesian Network Classifier-BayesNet)

BayesNet sınıflandırıcıları, sınıflandırma problemleri için tasarlanmış özel Bayes ağ türleridir. Denetimli sınıflandırma olarak nitelendirilen BayesNet, bir dizi tahmin değişkeni veya özelliği tarafından tanımlanan örneklerle etiketler veya kategoriler atamayı amaçlamaktadır.

Örneklere etiket atayan bu sınıflandırma modelinde, etiketlenmiş örnekleri içeren bir veri kümesinden otomatik olarak veya elle oluşturulmaktadır. Bayes teoremine göre çalışan BayesNet, belirsiz bilginin açık, grafiksel ve yorumlanabilir bir temsilini sunmaktadır. Bayes teoremi temelde birbirinden çok farklı olaylara bağlı olasılık hesabına dayanmaktadır. Bu teorem birbirinden bağımsız  $A$  ve  $B$  olaylarının eş zamanlı meydana gelme olasılığı, iki olayın olasılıklarının birbirleriyle çarpımına eşit olarak ortaya çıkmaktadır. Birbirine bağlı olaylar için bu olasılık 3.5 denkleminde verildiği şekilde elde edilmektedir [114]:

$$P(A \wedge B) = P(A) * P(A|B) \quad (3.5)$$

Tahmin, anormali tespiti, teşhis, otomatik içgörü, muhakeme, zaman serisi tahmini ve belirsizlik altında karar verme dâhil olmak üzere çok çeşitli görevler için kullanılabilen BayesNet'in verildiği 3.5 denklemi  $A$  ve  $B$  olaylarının birlikte olma ihtimalini verir. Bu denklemden yola çıkıldığı zaman  $P(A|B)$ ,  $B$  duruma ait sonucun bilinmesi halinde  $A$

durumunun meydana gelme olasılığını vermektedir. Bu durumda Bayes teoremi Denklem 3.6'da verildiği gibi formülarize edilebilir [114].

$$P(A \wedge B) = P(A) * P(A|B) = P(B) * P(A|B) \quad (3.6)$$

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

Olasılıksal bağımsızlık ile temsil ve akıl yürütme üzerine temel çalışmalara dayanan BN ile zor problemler verimli ve güvenilir bir şekilde çözülebilmesi amacıyla var olan yöntemlerin geliştirilmesi ile ortaya çıkmıştır. BayesNet algoritmasının Denklemi 3.7'de verildiği şekilde kullanılmaktadır [111].

$$P(A) \prod_{i=0}^{n-1} p(x_i|\pi_i) \quad (3.7)$$

Karmaşık sistemlerin modellenmesini pratik hale getirerek büyük alanları temsil etmenin sezgisel ve verimli bir yolunu sunmaktadır. BayesNet, belirsiz modellerde belirsizliği temsil etmek için uygun ve tutarlı bir yol sağlamaktadır ve belirsiz bilgiyi temsil etmek için giderek daha fazla kullanılmaktadır.

### 3.1.8. Naive Bayes Sınıflandırıcısı (Naive Bayes Classifier-NB)

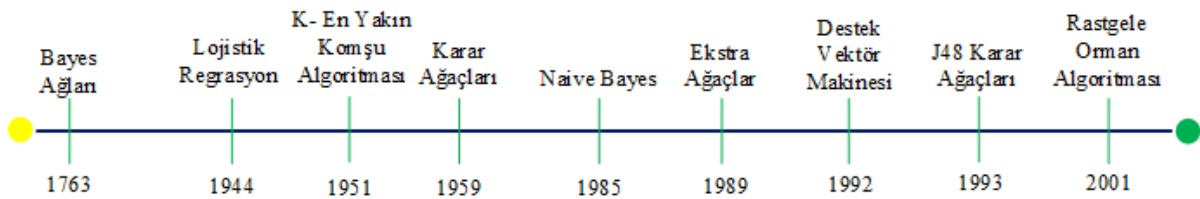
Bir olayın bağımsızlığını tahmin etmek için Bayes teoremini kullanan bir sınıflandırma algoritmasıdır. Hem iki sınıflı hem de çok sınıflı sınıflandırma problemlerinde kullanılan bir sınıflandırma algoritması olarak karşımıza çıkan NB, her bir sınıfa ait her özelliğin olasılıklarının tahmin için kullanıldığını ve belirli bir sınıf değerine ait her özelliğin olasılığının diğer özelliklerden bağımsız olduğunu varsaymaktadır. Özelliğin bilinen değeri için koşullu olasılık, her sınıfın örnek olasılıkları hesaplanarak ve en yüksek olasılık sınıfı değeri seçilerek elde edilebilmektedir. Büyük veri setleri için kullanıma çok uygun olan NB, Denklem 3.8'de gösterildiği gibi formülarize edilmektedir [67, 69].

$$P \frac{y}{x} = \frac{P(y) \prod_{i=1}^n P(\frac{x_i}{y})}{P(x)} \quad (3.8)$$

NB, daha karmaşık yöntemlerle karşılaştırıldığında son derece hızlı olarak öne çıkmaktadır. Denklemden de anlaşılacağı üzere sınıf koşullu özellik dağılımlarının ayrıştırılması, her dağılımın bağımsız olarak tek boyutlu bir dağılım olarak tahmin edilebileceği anlamına gelmekte; bu durum da, boyutsallık probleminden kaynaklanan sorunları hafifletmeye yardımcı olmaktadır. Bu nedenle de büyük boyutlu veri kümelerinin sınıflandırılmasında önemli bir rol oynamaktadır. NB ile sınıflandırma yapılırken belirli bir miktar öğretilmiş veri sisteme dâhil edilir. Burada önemli nokta sunulan verilere ait kategorilendirmelerin yapılmış olmasıdır. Öğrenmiş verilerde olasılık işlemleri yapılarak test verisinin dâhil olması ile önceki olasılık oranlarına göre işletme gerçekleştirilerek verinin kategorisini tahmin etmeye çalışılır. Önemli olan husus ise sisteme en başta verilen öğrenmiş veri setinin boyutunun büyük olmasıdır çünkü ne kadar çok öğrenirse sistem test verisi ile analizde daha doğru sonuçlar üretecektir. Çok farklı alanda kullanılmasının yanında verilerin sınıflandırma oranı ve yöntemi çok önemlidir [67, 69, 77, 97, 112].

### 3.1.9. J48 Karar Ağacı Sınıflandırıcısı (J48 Decision Tree Classifier-J48)

J48 karar ağacı algoritması, temeli C4.5 algoritmalarına dayanan, bir karar ağacı oluşturmak için kullanılan bir algoritmadır. Weka’da kullanılan bir sınıflandırma algoritması olan J48, istatistiksel bir sınıflandırıcı olarak nitelendirilmektedir. Bilginin her yönü, bir karara dayanmak için küçük alt gruplara bölünmektir. J48, bir öznitelik seçerek veriyi bölmenin gerçekten sonuçları olan standartlaştırılmış veri kazancına odaklanmaktadır. Özetlemek gerekirse, elde edilen aşırı standartlaştırılmış veri özniteliği kullanmaktadır. Küçük alt kümeler, algoritma tarafından döndürülmekte ve bir alt kümenin tüm durumlarda benzer bir sınıfa sahip bir yeri varsa, bölme işlemini durdurur. J48, sınıfın beklenen tahminlerini kullanarak bir karar düğümü geliştirmekte ve belirli özellikler, verilerin kayıp veya eksik öznitelik tahminleri ve değişen öznitelik maliyetleri ile ilgilenebilmektedir [97, 100, 101].



Şekil 3.6: Sınıflandırma yöntemleri geliştirme zaman çizelgesi

Sınıflandırma algoritmaları, belirli bir veri üzerinden yeni gelecek verilerin kategorisini belirlemeyen yarayan teknik olarak değerlendirilebilir. Sınıflandırmada, bir program verilen veri kümesinden veya gözlemlerden öğrenir ve ardından yeni gözlemi birkaç sınıf veya grup halinde sınıflandırır. Günümüzde birçok alanda ve farklı şekillerde kullanılması ile göze çarpan bu yöntemlerin geliştirme tarihleri çok önceki tarihlere dayanmaktadır. Şekil 3.6’da tez çalışmasında kullanılan yöntemlerin geliştirme yıllarına göre sıralanmasına yer verilmiştir.

Bu sınıflandırma algoritmaları temelde çok basit problemlerin çözülmesinde fayda sağlamaktadır. Ancak günümüzde teknolojik gelişmelerin önlenemez bir hızla artması sonucunda hemen hemen her alanda ve çok üst konfigürasyonlarla da kullanılabilir. Daha çok akademik çalışmalarla kendini gösterse de ticari ve kamu kuruluşları da kendi uygulamalarında bu yöntemleri kullanmaktadır. Bu tez çalışmasında; sınıflandırma yöntemlerinin kritik altyapıların korunmasında ve veri setleri üzerinde analiz yapmak amacıyla kullanılan çalışmalar ele alınarak bazı yöntemlere yer verilmiş olup bu bölümde söz konusu yöntemlerin genel mantıksal çerçevesine değinilmiştir.

### 3.2. KULLANILAN VERİ SETİ

Bu tez çalışmasında, gerçek hayattaki modern normal senaryoların yanı sıra ağ trafiğinden elde edilen verilerden ve çeşitli saldırı aktivitelerinden oluşan “UNSW\_NB15 Dataset” kullanılmıştır. Söz konusu veri seti Avustralya’daki “University of New South Wales”de IXIA PerfectStorm aracı tarafından hazırlanmış normal ve anormal ağ etkinliklerini barındırmaktadır.

Bu veri kümesi, saldırıların ve normal sınıfların benzer davranışlara sahip olduğu özellikleri içerdiğinden KDD'99 veri setinden daha karmaşıktır. Tcpdump aracı ham trafiğin 100 GB’ını yakalamak için kullanılır. Eğitim ve test setleri aynı dağılıma sahip olduğu UNSW-NB15 için özelliklerin korelasyonu denilebilmektedir.

Veri setindeki toplam örnek sayısı 2.540.044’tür. Bu veri kümesinin eğitim ve test veri kümelerinden oluşan ve 257.673 örnek içeren bir alt kümesi yapılandırılmıştır. Eğitim seti 175.341 örnek, test seti ise 82.332 örnek içermektedir. Veri kümesi: “Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode ve Worms” olmak üzere dokuz tür saldırı ve Normal aktivitelerden oluşan kategori ile toplamda 10 kategori içermektedir. Argus ve BroIDS log toplama araçları kullanılarak oluşturulmuş, 12 model geliştirilmiştir. Bu veri setine ait örneklerde 49 adet özellik bulunmakta olup öznitelikler: zaman özellikleri, akış özellikleri, içerik özellikleri ve ek özellikler olacak şekilde ayrı gruplardan oluşmaktadır. Tablo

3.1’de tez çalışmasında kullanılan veri setinin sütunlarına ve açıklamalarına yer verilmiş olup Tablo 3.2’de ise bu veri setinin diğer sütunlarına ve açıklamalarına yer verilmiştir.

**Tablo 3.1:** UNSW-NB15 veri seti alanları

| S.N. | SÜTUN ADI | AÇIKLAMASI                                | S.N. | SÜTUN ADI    | AÇIKLAMASI                                                        |
|------|-----------|-------------------------------------------|------|--------------|-------------------------------------------------------------------|
| 1    | srcip     | Kaynak IP Adresi                          | 18   | dpkts        | Hedeften Kaynağa Paket Sayısı                                     |
| 2    | sport     | Kaynak Port Numarası                      | 19   | swin         | Kaynak TCP Penceresi İlan Değeri                                  |
| 3    | dstip     | Hedef IP Adresi                           | 20   | dwin         | Hedef TCP Penceresi İlan Değeri                                   |
| 4    | dsport    | Hedef Port Numarası                       | 21   | stcpb        | Kaynak TCP Baz Sıra Numarası                                      |
| 5    | proto     | Transfer Protokolü                        | 22   | dcpb         | Hedef TCP Baz Sıra Numarası                                       |
| 6    | state     | Durumu ve Bağlı Olduğu Protokol           | 23   | smeansz      | Kaynak Tarafından İletilen Paket Boyutu Ortalaması                |
| 7    | dur       | Toplam Süre                               | 24   | dmeansz      | Hedef Tarafından İletilen Paket Boyutu Ortalaması                 |
| 8    | sbytes    | Kaynaktan Hedefe İletilen Byte            | 25   | trans_depth  | HTTP istek/yanıt İşleminin Veri Hattı Derinliği                   |
| 9    | dbytes    | Hedeften Kaynağa İletilen Byte            | 26   | res_body_len | HTTP Servisi Sunucularından Aktarılan Verilerin Gerçek Boyutu     |
| 10   | sttl      | Kaynaktan Hedefe Geçen Zaman              | 27   | sjit         | Kaynak Gecikmesi                                                  |
| 11   | dttl      | Hedeften Kaynağa Geçen Zaman              | 28   | djit         | Hedef Gecikmesi                                                   |
| 12   | sloss     | Kaynak Paketlerinin İletilip İletilmediği | 29   | stime        | Kayıt Başlangıç Zamanı                                            |
| 13   | dloss     | Hedef Paketlerinin İletilip İletilmediği  | 30   | ltime        | Son Kayıt Zamanı                                                  |
| 14   | service   | Kullanılan Servis                         | 31   | sintpkt      | Kaynak Paketler Arası Varış Süresi                                |
| 15   | sload     | Kaynak Bit Miktarı (1 Saniyede)           | 32   | dintpkt      | Hedef Paketler Arası Varış Süresi                                 |
| 16   | dload     | Hedef Bit Miktarı (1 Saniyede)            | 33   | tcprtt       | TCP Bağlantı Kurulumu Gidiş-Dönüş Süresi                          |
| 17   | spkts     | Kaynaktan Hedefe Paket Sayısı             | 34   | synack       | TCP Bağlantı Kurulum Süresi/SYN-SYN ACK Paketleri Arasındaki Süre |

**Tablo 3.2:** UNSW-NB15 veri seti alanları (devam)

| S.N. | SÜTUN ADI        | AÇIKLAMASI                                                                 |
|------|------------------|----------------------------------------------------------------------------|
| 35   | ackdat           | TCP Bağlantı Kurulum Süresi/SYN-SYN ACK Paketleri Arasındaki Süre          |
| 36   | is sm ips ports  | Kaynak ve Hedef IP Adresileri ve Bağlantı Noktası Numaraları Eşitmi (1/0)  |
| 37   | ct state ttl     | Kaynak/Hedef İletim Süresi İçin Belirlenen Değer                           |
| 38   | ct flw http mthd | HTTP Servisinde Get/Post Gibi Yöntemleri Olan Bağlantı Sayısı              |
| 39   | is ftp login     | FTP Oturumuna Kullanıcı Adı ve Şifre İle Erişiliyor Mu (1 veya 0)?         |
| 40   | ct ftp cmd       | FTP Oturumunda Komutu Olan Bağlantı Sayısı                                 |
| 41   | ct srv src       | Son 100 Bağlantıda Aynı Servisi ve Kaynak Adresini İçeren Bağlantı Sayısı  |
| 42   | ct srv dst       | Son 100 Bağlantıda Aynı Servisi ve Hedef Adresini İçeren Bağlantı Sayısı   |
| 43   | ct dst ltm       | Son 100 Bağlantıda Aynı Hedef Adresinin Bağlantı Sayısı                    |
| 44   | ct srv ltm       | Son 100 Bağlantıda Aynı Kaynak Adresinin Bağlantı Sayısı                   |
| 45   | ct src dport ltm | Son 100 Bağlantıda Aynı Kaynak Adresinin ve Hedef Portunun Bağlantı Sayısı |
| 46   | ct src sport ltm | Son 100 Bağlantıda Aynı Hedef Adresinin ve Kaynak Portunun Bağlantı Sayısı |
| 47   | ct dst src ltm   | Son 100 Bağlantıda Aynı Kaynak ve Hedef Adresine Ait Bağlantı Sayısı       |
| 48   | attack cat       | Her Saldırı Kategorisinin Adı                                              |
| 49   | label            | Saldırı mı/Normal Mi (1 veya 0)?                                           |

### 3.3. VERİ SETİNDE YER ALAN SALDIRI TÜRLERİ

#### 3.3.1. Fuzzer Saldırıları

Bu saldırılar, davetsiz ve kötü niyetli bir istemci tarafından, sistemi tehlikeye atmak için büyük miktarda veriyi dâhil ederek işletim sistemi, uygulama veya herhangi bir ağ ortamı gibi herhangi bir platformdaki güvenlik kusurlarını bulmaya çalışmasıyla gerçekleşmektedir. Temel amaç, uygulamada güvenlik açıklarını bulmak için otomatik bir şekilde yapılan işlemidir. Saldırının kapsamı, kaynak koduna büyük miktarda rastgele veri veya fuzz eklemekten ve sonuçları gözlemlemekten oluşmaktadır. Bilgi veya değerlendirme gerektirmeyen, düşük maliyetli ve zaman kazandıran yetenekleri nedeniyle yaygın olarak kullanılmaktadır [77, 82]. Bir fuzzing saldırısı ile kötü niyetli siber saldırganlar tarafından, kod eklemeye veri almaya eğilimli alanları tespit edilir, uygulamaları ciddi bir uygulama saldırısı tehlikesiyle karşı karşıya bırakılır [89, 90, 95].

#### 3.3.2. Analysis (Analiz) Saldırıları

Bu tür saldırılar, web uygulamalarına, e-posta kullanıcı sistemine veya Hiper Metin İşaretleme Dili (HyperText Markup Language-HTML) dosyalarına sızmak için bağlantı noktaları, e-postalar veya web komut dosyaları aracılığıyla gerçekleştirilen saldırı türüdür [77, 82].

### 3.3.3. Backdoor (Arka Kapı) Saldırıları

Bu saldırılar, bir davetsiz misafirin yetkisiz uzaktan erişim kullanarak yasadışı bir şekilde bir sistemi işgal etmeye çalıştığı ve bir komutun son yürütülmesine kadar kendisini fark edilmeden tutmasıyla gerçekleşmektedir. Bilgisayar korsanları, kötü amaçlı yazılım kullanarak, yazılım açıklarınızdan yararlanarak veya hatta doğrudan cihazın donanımına/ürün yazılımına bir arka kapı yükleyerek cihazınıza bir arka kapı kurabilmektedir. Bu saldırı türünde hedef: izleme, veri hırsızlığı, kripto hırsızlığı, sabotaj amaçlı yapılabilmektedir [89, 100, 95].

### 3.3.4. Hizmet Reddi (Denial of Service-DoS) Saldırıları

Bu tür saldırılar, yasal kullanıcının sisteme erişimini durdurmak için bilgisayar kaynaklarına sürekli erişerek sistemi bozmaya çalışmaktadır. Kötü niyetli bir aktörün, cihazın normal işleyişini kesintiye uğratarak bir bilgisayarı veya başka bir cihazı hedeflenen kullanıcılar tarafından kullanılamaz hale getirmeyi amaçladığı bir tür siber saldırıdır. DoS saldırıları tipik olarak, normal trafik işlenemeyecek duruma gelene kadar hedeflenen bir makineyi isteklerle doldurarak veya bu makineye ek kullanıcılara hizmet reddi ile sonuçlanarak çalışır [77, 82, 92]. Bir DoS saldırısı, saldırıyı başlatmak için tek bir bilgisayar kullanılmasıyla karakterize edilir. İki türlü yapılabilmektedir. Birincisi: bir makinenin tüm kullanılabilir sabit disk alanını, belleği veya Merkezi İşlem Birimi (Central Process Unit-CPU) zamanını tüketmesine neden olabileceği şekildedir. İkincisi ise: kötü niyetli aktörün, hedeflenen sunucuyu fazla miktarda paketle doyurarak, sunucu kapasitesini aşırı doyurması ve hizmet reddine neden olmasıyla gerçekleşebilir. DoS saldırılarının başarılı olması için, kötü niyetli aktörün hedeften daha fazla kullanılabilir bant genişliğine sahip olması gerekmektedir [89, 95, 116].

### 3.3.5. Exploit (İstismar) Saldırıları

Bu saldırı ile teknik bir engel, hata veya hatalardan yararlanmaya çalışılmaktadır. Bu nedenle sistemin kurbanı olan kullanıcı, saldırıdan tamamen habersizdir. Bilgisayar korsanlarının sisteme erişmesini sağlamak için yazılım açıklarından (genellikle tarayıcılar, Adobe Flash, Java vb. web'e yönelik yazılımlarda) yararlanan saldırılardır. İstismarlar çeşitli şekillerde gerçekleşebilse de, yaygın olarak, kötü amaçlı web sitelerinden başlatılmasıyla oluşmaktadır. Kullanıcının kötü amaçlı siteyi kazara ziyaret etmesi, bir kimlik avı e-postası alması veya bir reklam içindeki kötü amaçlı sitenin bağlantısını tıklaması ile hedef olabilmektedir [77, 82, 95].

### 3.3.6. Generic (Genel) Saldırıları

Bu saldırı, blok şifresinin konfigürasyonuna bakılmaksızın bir çakışmaya sebep olmak için her blok şifresine karşı karma işlevi kullanan bir yöntem olarak gerçekleştirilebilmektedir [77].

### 3.3.7. Reconnaissance (Keşif) Saldırıları

Keşif saldırısı, bir saldırganın gerçek bir saldırı başlatmadan önce hedef hakkında tüm olası bilgileri toplamak için kullandığı bir güvenlik saldırısıdır. Saldırgan, gerçek bir saldırı için hazırlık aracı olarak keşif saldırısını kullanmaktadır. Keşif saldırılarının en yaygın örnekleri arasında paket koklama, ping süpürme, bağlantı noktası tarama, kimlik avı ve sosyal mühendislik sayılabilmektedir [77, 90].

### 3.3.8. Shellcode (Kabuk Kodu) Saldırıları

Shellcode, bilgisayar korsanlarının çeşitli yazılım açıklarından yararlanmak için kullandıkları, uzaktan sisteme enjekte edilen özel bir kod türüdür. Saldırganların saldırı sonucunda etkilenen sistemin kontrolünü ele geçirebileceği bir komut kabuğu ürettikleri için bu şekilde adlandırılmıştır. Bu tür kodlar, ana makineyi tehlikeye atmak için kabuktan bir sisteme girmeye çalışmaktadır [82, 95].

### 3.3.9. Worm (Solucan) Saldırıları

Solucan, hızla çoğalabilen ve bir ağ içindeki cihazlara yayılabilen bir tür kötü amaçlı yazılım veya kötü amaçlı yazılım olarak tanımlanmaktadır. Yayıldıkça, bant genişliğini tüketmekte olup, virüslü sistemleri aşırı bir şekilde şişirmekte ve onları güvenilirmez veya kullanılamaz hale getirmektedir. Dosyaları değiştirebilir ve silebilir yapıda olan solucanlar, bilgisayar kaynaklarına daha fazla zarar vermek amacıyla kendilerini kopyalamaya çalışmaktadırlar [77, 82, 90].

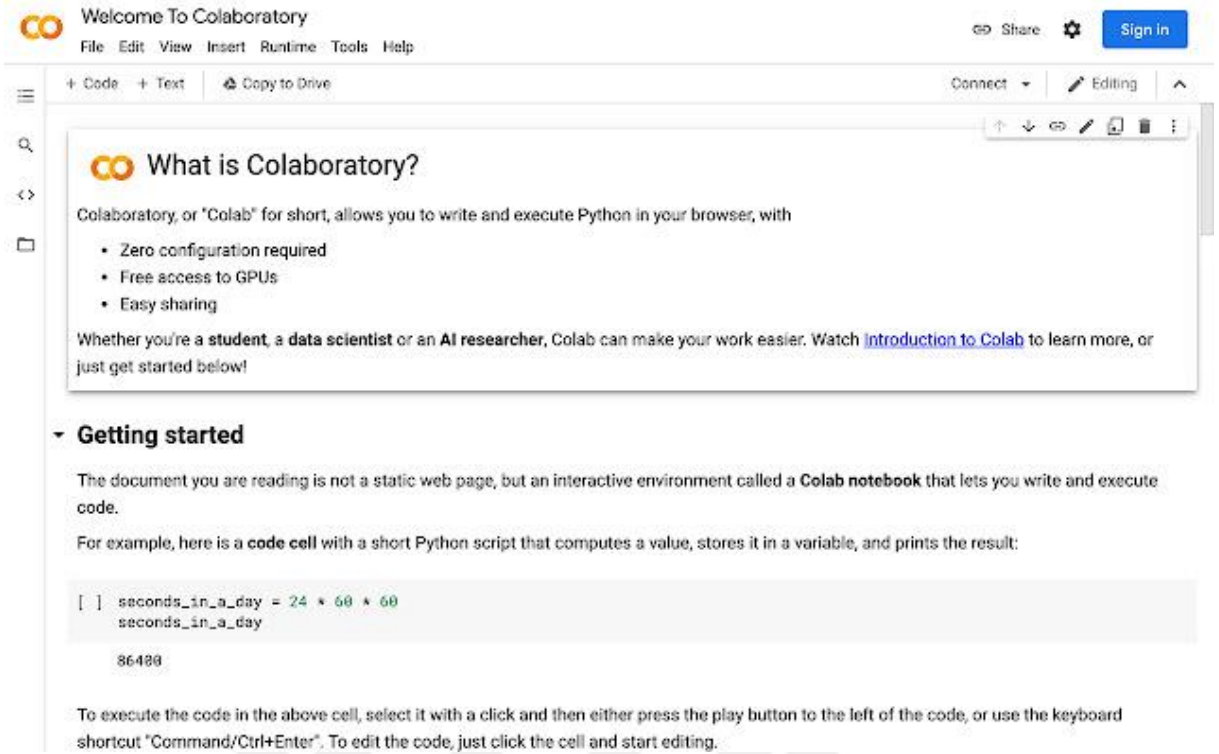
## 3.4. KULLANILAN ARAÇLAR VE GELİŞTİRME ORTAMI

Komutlar, bir sistemin, programın veya makinenin belirli yönlerini kontrol etmeye yarayan sistematik yöntemlerdir. Programlama dilleri, komutları kontrol eden sınıfları ve işlevleri kullanmaktadır. Programlamanın bu kadar önemli olmasının nedeni, bir bilgisayarı bu komutları tekrar tekrar tamamlamaya yönlendirmesidir, böylece insanlar görevi tekrar tekrar yapmak zorunda kalmamakta; yapacakları işi bu vasıta ile hızlı ve kolay bir şekilde yapmaktadır. Programlama dilleri, yinelenen ve sistematik görevler oluşturmaya yarayan farklı

ifade türlerini ve mantıksal yapılandırma kurallarını ifade etmektedirler. Bu diller çok çeşitlidir ve her biri farklı türdeki gereksinimlere yönelik olarak geliştirilmişlerdir. Ancak temelde alt, orta ve yüksek seviyeli programlama dilleri olmak üzere üç sınıfa ayrılmaktadır. Günümüzde hayli popüler hale gelen Python programlama dili, artık en popüler programlama dillerinden biri olmuştur. Özellikle veri bilimciler tarafından 2019 yılında yapılan anket çalışmalarında, talep edilen ilk 15 teknoloji arasında Python'un ilk sırada yer aldığı ve açık ara farkla en sık kullanılan dil olarak kendini gösterdiği kanıtlanmıştır. Finans ve bankacılık alanındaki birçok profesyonel veri bilimi alanlarında da Python'un, diğer araç ve dillerin önüne geçtiği görülmektedir. Python, öğrenmesi, hata ayıklaması kolay, yaygın olarak kullanılan, nesne yönelimli, açık kaynaklı, yüksek performanslı bir dildir. Ayrıca Python, programcılar tarafından her gün problem çözmede kullanılan veri bilimi için olağanüstü kütüphanelere sahiptir. Python'un en yaygın kullanımlarından biri, veri yapılarını hızlı bir şekilde oluşturma ve yönetme yeteneğidir. Çünkü veri yapılarını ve karmaşık veri kümelerini işlemek, analiz etmek ve hatta temsil etmek için çok sayıda araç sunmaktadır. Bu tez çalışmasında temel olarak bu nedenlerden dolayı Python programlama dili kullanılmıştır [106].

Python programlama dili ile geliştirilmek istenen çalışmada uygulama geliştirme ortamı olarak Google Colabratory (Colab) seçilmiştir. Colab, temelde tamamen bulutta çalışan ücretsiz bir Jupyter notebook ortamıdır. En önemli özelliği ise, Colab bir kurulum gerektirmemekte, ayrıca oluşturacak not defterleri birçok kişi tarafından eş zamanlı olarak düzenlenebilmektedir.

Öne çıkan bir diğer avantajı ise, Colab'ın not defterine kolayca yüklenebilen en popüler makine öğrenimi kütüphanelerini desteklemesidir. Veri biliminde bir geliştirici olarak Colab'ı kullanarak çevrimiçi olarak bir program ya da uygulama yüklemeyen, Python'da kod yazılıp yürütülebilmekte; cep telefonu ile dahi not defterleri oluşturulup geliştirme yapılabilir [106-108]. Kısacası Colab'ı kullanmak için bir Google hesabının olması yeterli olmaktadır. Bu amaçla geliştirme ortamı olarak Colab tercih edilmiştir. Şekil 3.7'de Colab'ın arayüzüne yer verilmiştir.



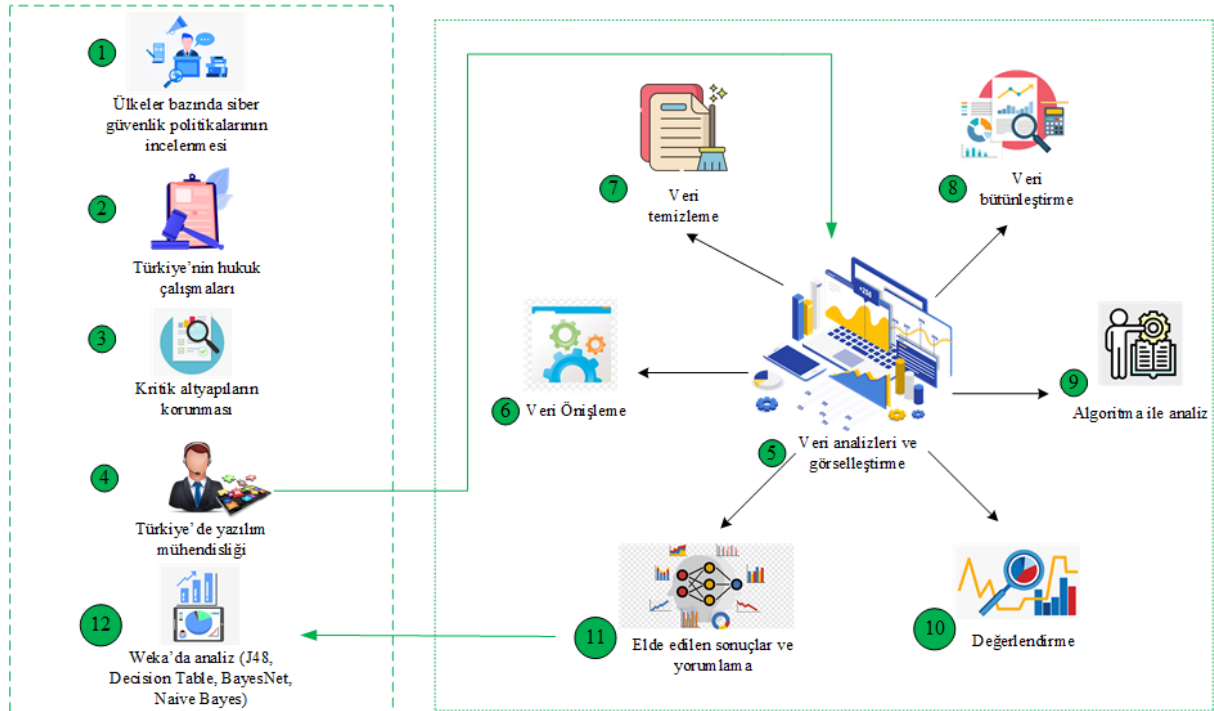
Şekil 3.7: Google Colabratory arayüzü [107]

Weka, Yeni Zelanda'daki Waikato Üniversitesi tarafından geliştirilen bir veri madenciliği algoritması uygulamasıdır. Weka, GNU Genel Kamu Lisansı altında yayınlanan açık kaynaklı bir yazılımdır. Weka, veri ön işleme, makine öğrenimi algoritması uygulama ve görselleştirme için araçlar içermekte olup makine öğrenimi tekniklerinin oluşturulmasına ve bunları gerçek dünyadaki veri madenciliği sorunlarına uygulamaya olanak tanımaktadır. Veri ön işleme, kümeleme, sınıflandırma, regresyon, görselleştirme ve özellik seçimi, Weka'nın desteklediği tipik veri madenciliği faaliyetlerinden sadece birkaçı olarak öne çıkmaktadır.

Weka'nın stratejilerinin tümü, verilere tek bir düz dosya veya her veri noktası için sabit sayıda öznitelik ile bağlantı olarak erişilebilir olduğu önermesine dayanmaktadır. Bir Grafik Kullanıcı Arayüzü (Graphical User Interface-GUI) ile birlikte gelen Weka'ya; ARFF, CSV' ve C4.5 formatında veriler, dosyalar, Tekdüzen Kaynak Bulucu (Uniform Resource Locator-URL)'lar ve veri tabanları dâhil olmak üzere çeşitli kaynaklardan yüklenebilmektedir [110]. Weka'nın tüm bu özelliklerinin yanında madenciliği ve makine öğrenimi için birçok farklı algoritma sunması, verilerin görselleştirilme imkânı sağlaması ve platform bağımsız yapıda olmasından dolayı bu tez çalışmasında tercih edilmiştir.

### 3.5. GERÇEKLENEN SİSTEM

Günlük (log) dosyası, bilgisayarın veya sistemin olayların listesini, sistemle ilgili bilgileri içeren kayıtlardır. Log dosyasına kaydedilen veriler: uygulamalar, hizmetler, sistem hataları ve çekirdek mesajları hakkında bilgiler içermektedir. Log dosyaları genellikle yazılım yüklemeleri sırasında ve web sunucuları tarafından oluşturulur, ancak çeşitli başka amaçlar için de kullanılabilirler. Sistemin veya bilgisayarın başladığı andan sonlandırıldığı ana kadar gerçekleşen her eylemi kaydetmektedir. Log dosyaları, ağ gözlemlenebilirliği için en önemli veri kaynağıdır. Log dosyası, bir işletim sistemi, uygulama, sunucu veya başka bir cihaz içindeki kullanım kalıpları, etkinlikler ve işlemler hakkında bilgileri de içermektedir. Log analizi ise, log kayıtlarını gözden geçirme, yorumlama ve anlama sürecidir. Log dosyalarını bir bilgi işlem ortamından toplamak ve analiz etmek için SIEM veya başka bir analiz aracı kullanılabileceği gibi yazılım geliştiriciler tarafından hazırlanan web tabanlı veya masaüstü uygulaması tarafından da analizler yapılabilmektedir. Bu bölümde, tez çalışmasının uygulama aşamasında veri setinin bir değerlendirmesi, kullanılan kütüphaneler, işlem adımları detaylı bir şekilde açıklanmaktadır. Ayrıca her bir işlem adımı üzerinden gerçekleştirilen işlemler ve adımlar açıklanmaktadır.

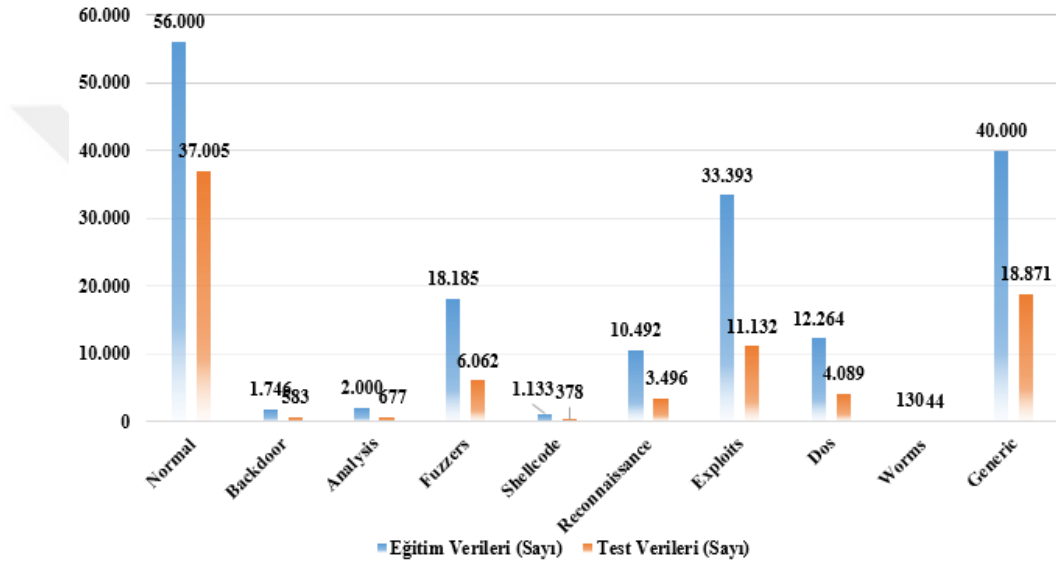


Şekil 3.8: Tez çalışmasının genel içerik diyagramı

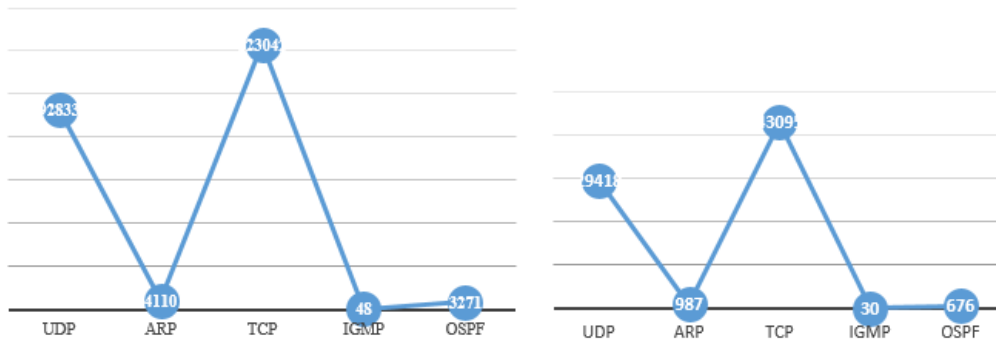
Şekil 3.8’de bu tez çalışmasında yapılan çalışmalara ait içerik diyagramı yer almaktadır. Diyagramda verilen 4. adıma kadar olan aşama yani bu bölüme kadar olan genel araştırmalar yer verilmiştir. Sonraki bölümlerde ise uygulamaya yönelik içerikler sunulacaktır.

### 3.5.1. Veri Seti Değerlendirmesi

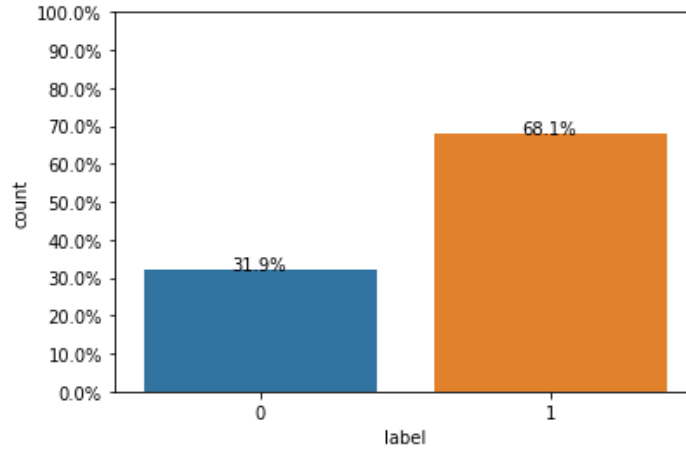
Şekil 3.9’da veri setinde yer alan saldırı türlerinin eğitim ve test veri setindeki dağılımları yer almaktadır. , Şekil 3.10’da ise veri setinde eğitim ve test veri setlerindeki protokol dağılımı gösterilmiştir.



Şekil 3.9: Veri setinin saldırılara göre dağılımı



Şekil 3.10: Eğitim ve test veri setlerindeki protokol dağılımı



**Şekil 3.11:** Eğitim veri setindeki normal ve saldırı verilerinin oranları

Şekil 3.11’de uygulamada kullanılan eğitim veri setindeki normal ve saldırı verilerinin oranları sunulmuştur.

### 3.5.2. Kullanılan Kütüphaneler

Bu bölümde uygulamanın tümünde kullanılan başlıca önemli kütüphanelere yer verilmiştir. Ön işleme, dönüştürme, değiştirme ve sınıflandırma gibi aşamalarda kullanılan bu kütüphaneler Tablo 3.3’de gösterilmiştir.

**Tablo 3.3:** Kullanılan başlıca kütüphaneler

| S.N. | KÜTÜPHANE ADI  | S.N. | KÜTÜPHANE ADI          |
|------|----------------|------|------------------------|
| 1    | numpy          | 12   | LogisticRegression     |
| 2    | pandas         | 13   | SGDClassifier          |
| 3    | matplotlib     | 14   | LinearSVC              |
| 4    | seaborn        | 15   | MultinomialNB          |
| 5    | scipy          | 16   | DecisionTreeClassifier |
| 6    | pickle         | 17   | RandomForestClassifier |
| 7    | PrettyTable    | 18   | GridSearchCV           |
| 8    | warnings       | 19   | RandomizedSearchCV     |
| 9    | StandardScaler | 20   | cross_validate         |
| 10   | LabelEncoder,  | 21   | cross_val_predict      |
| 11   | OneHotEncoder  | 22   | apriori                |

Python, günümüzde en çok kullanılan programlama dillerinin başında gelmektedir. Bu başarı, genellikle diğer programlama dilleriyle karşılaştırıldığında yüksek verimliliğine ve kodlamaya yeni başlayanlar için bile öğrenmesi ve kullanımı kolay olmasından

kaynaklanmaktadır. Ancak Python'un en faydalı özelliklerinden biri de çok sayıda açık kaynak kütüphaneye sahip olmasıdır. Veri bilimi ve görselleştirmeden görüntü ve veri manipülasyonuna kadar her şeyde kullanılabilir. Python kütüphaneleri, ML ve DL alanında da çok sayıda bulunmaktadır. Colab'da da bu tarz birçok Python kütüphanesi bulunmaktadır. Bu kütüphaneler ile çok rahat ve geniş bir çerçevede analizler yapılabilmektedir.

### 3.5.3. Uygulanan Yöntem ve Ön İşleme

Veri ön işleme, veri madenciliği ve veri analizi sürecinde ham verileri alan ve onu bilgisayarlar ve makine öğrenimi yöntemleri tarafından anlaşılabilen ve analiz edilebilen bir formata dönüştüren bir adım olarak değerlendirilmektedir. Bu aşama analiz adımlarının en önemlilerindendir. Sağlıklı ve uygun bir ön işleme gerçekleştirmek başarımı büyük oranda artıracaktır. Bu aşamada metin ve görüntü biçimindeki yapılandırılmamış veriler, analizden önce önce temizlenmeli ve biçimlendirilmelidir. İşlenmiş veriler, en güçlü algoritmalarla bile daha önemlidir; öyle ki, kötü verilerle eğitilen makine öğrenimi modelleri, yapmaya çalışılan analiz için gerçekten zararlı olabilmekte ve anlamsız sonuçlar verebilmektedir. Veriler uygun şekilde ön işleme tabi tutulduğunda ve temizlendiğinde, çok daha kolay ve doğru sonuçlar elde edilebilir.

Bu tez çalışmasında, gerçek hayattaki modern normal senaryoların yanı sıra ağ trafiğinden elde edilen verilerden ve çeşitli saldırı aktivitelerinden oluşan “UNSW\_NB15 Dataset” analiz edilmiştir. Veri setinde normal ve anormal ağ etkinlikleri yer almaktadır.

Toplam örnek sayısı 2.540.044 olan veri seti, 257.673 örnek içeren bir alt küme şeklinde yapılandırılmıştır. Eğitim seti 175.341 örnek, test seti ise 82.332 örnek içermektedir. Çalışmadaki amaç: “Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode ve Worms” olmak üzere dokuz tür saldırı ve Normal aktivitelerin bir analizi gerçekleştirmek ve birçok sınıflandırma algoritmaları ile bu analiz sonucunda en sağlıklı sınıflandırma metodolojisini elde etmek olmuştur. Bu veri setine ait örneklerde 49 adet özellik bulunmakta olup öznitelikler: zaman özellikleri, akış özellikleri, içerik özellikleri ve ek özellikler olacak şekilde toplam ayrı gruptan oluşmaktadır.

Çalışmada, öncelikle kütüphanelerin aktarılması sağlanmıştır. Bu kütüphaneler Tablo 3.3'de gösterilmiştir. Veri kümesi, eksik değerler vb. gibi mevcut sorunların üstesinden gelmek için oluşturulmuştur. Veri analizi ve görselleştirme yapılarak, özellikleri daha iyi anlamak için verilerdeki kalıpları analiz etmek ve bulmak için veri görselleştirme teknikleri kullanılmıştır. Verilerin nasıl dağıtıldığını, bir özelliğin diğeriyle nasıl ilişkilendirildiği ve veri kümesinde

hangi anormalliklerin olduğu hakkında bilgi edinmek için bir takım çalışmalar yapılmıştır. Kullanılan veri seti, klasik KDD veri setinin geliştirilmiş modern bir alternatiftir, KDD veri seti güncelliğini yitirmiştir ve birçok anomaliye sahiptir. UNSW-NB15 veri kümesi, izinsiz giriş tespiti için mevcut diğer veri kümelerine kıyasla sınıf açısından daha dengelidir. UNSW-NB15 veri seti, diğerlerine kıyasla boyut olarak daha küçük, ancak daha az yedekli olmasına rağmen, bir modeli yüksek doğrulukta eğitmek için yeterlidir.

Veri ön işleme, model oluşturma için makine öğreniminde ilk adımdır. Sistem tarafından toplanan veriler genellikle tutarsızdır, ön işleme ile verileri görselleştirme ve analiz adımıyla hazırlanmaktadır. Gerçekleştirilen ilk çalışma veri temizleme için analizler yapılmış olup veri setinde eksik değerler bulunamamıştır. Her bir özelliğin açıklaması incelenmiş, veriler çarpık olduğu için görselleştirmeden önce normalleştirilmesi gerekli olmuştur. İlk olarak, bu öznitelikteki benzersiz numaralandırma nedeniyle mükerrer kayıtlar tanımlanamadığından, “id” özniteliği her iki veri kümesinden de çıkarılmıştır. Daha sonra, Pandas kütüphanesinin yerleşik işlevlerini kullanarak, veri kümelerindeki hem eğitim hem de test veri kümelerinden yinelenen veriler bulunmuş ve çıkarılmıştır. Ayrıca veri setindeki saldırı tiplerini içeren öznitelik ikili sınıflandırma problemlerinde gereksiz olduğu için kaldırılmıştır.

Kodlanmış değişkenler ve çıkarılan özellikler incelenmiş; yalnızca veri kümesinin boyutsallığını artırmış olduğu için öncelikle özellikler arasında ilişki çıkarılmıştır. Veri analizi adımıyla geçmeden önce, özelliklerin nasıl dağıtıldığını daha iyi anlayabilmek için veri kümesinden aykırı değerlerin kaldırılması sağlanmıştır.

PyCaret kütüphanesi, model eğitim sürecini basitleştirebilecek tüm gerekli işlev bloklarından veya modüllerden oluşan bir ardışık düzen oluşturmaktadır. Bu, veri ön işleme aşamasını da kapsamaktadır. Veri ön işleme ve veri hazırlama ile ilgili işlevler, kütüphanenin önemli bir bileşenidir. Bunun bir sonucu olarak, PyCaret kütüphanesi bu fonksiyonları otomatik olarak işleyebilmektedir. Geliştirici olarak yapılması gereken, kurulum fonksiyonunu çağırarak gerekli işlevleri ayarlamaktır. Veri kümesinde eksik olan değerlerle başa çıkmak için, PyCaret varsayılan olarak sayısal özellikler durumunda özelliğin ortalama değerini kullanmaktadır. Gerekirse manuel olarak bir medyan değeri de seçilebilmektedir ancak bu çalışmada medyan değerinin standart değer ile daha uygun sonuç verdiği görülmüştür.

Normalleştirme için PyCaret varsayılan olarak “zscore” kullanmaktadır ve dönüşüm için varsayılan olarak “yeo-johnson” yöntemi kullanılır. Özellikleri daha iyi anlamak için verilerdeki kalıpları analiz etmek ve bulmak için veri görselleştirme tekniklerini kullanılmıştır. Öngörülere dayanarak, eğitim sırasında veri kümesine dahil edilecek optimum özelliklerin neler

olabileceğine veya modelin doğruluğunu artırmak için hangi ilgili özelliklerin çıkarılabileceğine ilişkin ilerleyen aşamalar için gerekli kararlar alınmıştır.

Verilen veri seti için apriori algoritması kullanılarak birliktelik kuralı oluşturulmuş, güven ve artış sırasına göre sıralama yapılmıştır. Sıralamadan sonra hem öncülleri hem de sonuçları eklemek için her satırı yinelenmiştir. Bu işlemden sonra sıralama tekrar yapılarak liste oluşturulmuştur. Tüm veri kümesi için sık işlem sütunlarını bulunmuş, sık kullanılan öğelerin alt paketlerini bulmak için yine apriori algoritmasını kullanılmıştır. Kural, alt kümelerden oluşturulmuş, ayarlamak için ise her sık sütunu eklenmiştir. Tüm olası sütunları bulmak için veri kümesini yinelenmiş bir dizi oluşturulmuştur.

Bir takım küçük adımlardan sonra veri setinin alanlarından nominal olan alanların her biri “One Hot Encoding” kodlama yöntemi kullanılmıştır. Bu yöntemi kullanmaktaki amaç veri kümemizde metin verisi olan birkaç kategorik sütunun makine öğrenmesi modellerinin metin verilerini işleyemediği yalnızca sayıları işleyebilmesidir. One Hot Encoding, makine öğrenimi modelleri için kategorik özellikleri önceden işlemenin yaygın kullanılan bir yöntemidir. Bu kodlama türü, olası her kategori için yeni bir ikili özellik oluşturmakta ve her örneğin kendi orijinal kategorisine karşılık gelen özelliğine “1” değerini atamaktadır. Bu yöntem, öğrenme teknikleri eğitiminde özellik mühendisliği sürecinin oldukça önemli bir parçasıdır. Çünkü kategorik veriler işlenirken sayısal forma dönüştürülmelidir. Kodlama genellikle verilerin tamsayı gösterimine uygulanmaktadır. Burada tamsayı kodlanmış değişken kaldırılıp ve her benzersiz tamsayı değeri için yeni bir ikili değişken eklenmektedir. İşlem sırasında, etiket kodlanmış kategorik verilere sahip bir sütun almakta ve ardından sütunu birden çok sütuna bölmektedir. Sayılar, hangi sütunun hangi değere sahip olduğuna bağlı olarak rastgele “1”ler ve “0”larla değiştirilmektedir. Yöntem bazı sıralı durumlar için yararlı olsa da, bazı girdi verilerinin kategori değerleri için herhangi bir sıralaması yoktur ve bu, tahminlerle ve düşük performansla ilgili sorunlara yol açabilmektedir. “Label Encoding” yöntemi de benzer işlemi yapsa da bu yöntemin kategorilerin sıralı ve düzgün olduğu durumlarda kullanılması önerilmektedir. Bu yüzden önce kullanılmış sınıflandırmada daha düşük bir başarımla verildiği görülerek “One Hot Encoding” kodlama yöntemi kullanılmıştır. Daha sonra aynı işlemi test verilerine uygulayabilmemiz için tüm önemli parametreleri ve nesneleri diske kaydedilmiştir. Tüm yöntemler test veri setine de uygulanarak ön işlem aşamasının tamamlandığı düşünülmüştür. Veri ön işlemenin son adımı, özellik ölçeklendirmedir ve tüm veri kümesinin sayısal değerlerini standart bir ölçeğe dönüştürmek için yapılmaktadır. Özellik ölçeklendirme

işlemi, Scikit-Learn'de “MinMaxScaler” ve “StandardScaler” fonksiyonları kullanılarak gerçekleştirilmiştir.

### 3.5.4. Sınıflandırma

#### 3.5.4.1. Lojistik Regresyon ile Sınıflandırma

Yukarıdaki tüm ön işleme işlemlerinden sonra verileri eğitmek için temel olarak LR ile sınıflandırmaya başlanmıştır. LR, bağımlı bir kategorik hedef değişkeni tahmin etmek için kullanılan denetimli bir öğrenme algoritmasıdır. İkili sınıflandırma problemleri (iki sınıf değeri olan problemler) için başvurulmuş bir sınıflandırma yöntemidir. Hiperparametre olarak “alfa” ve “penalty” ayarlanmıştır. Her bir ML algoritması için özellik ölçekleme yöntemi, karşılaştırmalı analizden sonra performans metriklerine dayalı olarak seçilmektedir.

Kategorize edilmek istenen büyük veri setlerinde, avantaj sağlamaktadır; bu sebeple ilk olarak sınıflandırmada LR yöntemi kullanılmıştır. Bu yöntemde tahmin edilen değerleri olasılıklara eşlemek için kullanılan matematiksel bir fonksiyon olan “Sigmoid” fonksiyonu kullanılmıştır. “Sigmoid” bir gerçek değeri “0 ve 1” aralığında başka bir değere eşlemekte olup regresyonun değeri 0 ile 1 arasında olmak zorunda olduğu için bu sınırın ötesine geçememekte, bu nedenle "S" formu gibi bir eğri oluşturmaktadır. S-form eğrisi, Sigmoid fonksiyonu veya lojistik fonksiyon olarak adlandırılabilir. LR’de, 0 veya 1 olasılığını tanımlayan eşik değeri kullanılmıştır. Eşik değerinin üzerindeki değerler 1'e, eşik değerlerinin altındaki değerler 0'a eğilim göstermektedir.

Bu işlemler için veri seti iyi hazırlanmış ve eğitim setini kullanarak veri seti eğitilmiştir. Eğitim sağlamak veya modeli eğitim setine uydurmak için “Sklearn kütüphanesi” “LogisticRegression” sınıfının içine aktarılmıştır. Sınıfı içe aktardıktan sonra, bir sınıflandırıcı nesnesi oluşturulmuş ve modeli lojistik regresyona uydurmak için kullanılmıştır. Model eğitim seti üzerinde iyi eğitilmiştir, bu yüzden test seti verilerini kullanarak sonucu tahmin edilmiştir. Daha sonra sınıflandırmanın doğruluğunu kontrol etmek için karışıklık matrisini (Confusion Matrix-CM) oluşturulmuştur. Bunu oluşturmak için, sklearn kütüphanesinin concept\_matrix fonksiyonu dâhil edilmiştir. Fonksiyonu içe aktardıktan sonra, yeni bir değişken kullanılarak çağırılmıştır. Fonksiyon, gerçek değerler ve sınıflandırıcı tarafından hedeflenen değer dönüşü olmak üzere iki parametre almıştır. Sonucu görselleştirmek için “Matplotlib kütüphanesi” kullanılmıştır. LR için eğitim seti sonucunu başarılı bir şekilde görselleştirilmiştir ve bu sınıflandırmadaki amaç saldırı olan verilerle olmayanları ayırmaktır.

#### 3.5.4.2. *Extra Ağaçlar Sınıflandırıcısı İle Sınıflandırma*

XT, birden çok ağaç oluşturma ve özelliklerin rastgele alt kümelerini kullanarak düğümleri ayırması bakımından RF gibi değerlendirilebilir ancak iki önemli fark vardır. Bunlardan ilki gözlemleri önyüklemeyi ve düğümler, en iyi bölmelere değil, rastgele bölmelere ayrılmaktadır. Öncelikle birden çok varsayılan olarak ağaç oluşturulur, değiştirme düğümleri olmadan, her düğümde seçilen özelliklerin rastgele bir alt kümesi arasındaki rastgele bölünmelere göre tüm gözlemlerin rastgele bölünmelerinden oluşur. Sınıflandırmada “max\_depth”, “min\_samples\_split” ve “min\_samples\_leaf” için parametreler ayarlanmıştır. Ardından, çapraz doğrulama için girişler verilmiştir. İnşa edilecek ağaç sayısı tasarlandıktan sonra sınıflandırma modeli oluşturulmuş; sınıflandırma sağlanmıştır.

#### 3.5.4.3. *Destek Vektör Makineleri ile Sınıflandırma*

SVM hem sınıflandırma hem de regresyon problemleri için kullanılabilen denetimli bir makine öğrenme algoritmasıdır. Ancak genellikle sınıflandırma için kullanılmaktadır. 2 veya daha fazla etiketli veri sınıfı verildiğinde, tüm sınıfları ayıran optimal bir hiperdüzlem tarafından resmi olarak tanımlanan ayırt edici bir sınıflandırıcı görevi görmektedir. Daha sonra aynı alana eşlenen yeni örnekler, boşluğun hangi tarafına düştüklerine göre kategorilere ayrılabilir. SVM’de, hiperdüzlemin en yakın veri noktalarıdır, bir veri setini bölen hiperdüzlemin konumunu değiştirecek noktalarıdır.

Bu nedenle, bir veri kümesinin kritik öğeleri olarak kabul edilebilirler. Oluşan bu geometri bize bir hiperdüzlemin çevre uzayından bir boyuttan daha küçük bir alt uzay olduğunu göstermektedir. Örneğin, n-boyutlu bir uzayın hiperdüzlemi, n-1 boyutunda düz bir altkümedir. Doğası gereği alanı iki yarım mekâna ayırmaktadır. Sınıflandırıcımızı eğitmek için “Hinge Loss” adı verilen ve “Menteşe Kaybı” olarak da bilinen fonksiyon kullanılmıştır. Menteşe kaybı, "maksimum marj" sınıflandırması için, özellikle de SVM'ler için kullanılmaktadır.

Düzenleyici, marj maksimizasyonu ve kayıp arasında denge kurmaktadır. Herhangi bir veri noktasından maksimum derecede uzakta olan karar yüzeyini bulmak amaçlanmıştır. Buradaki hedef öğrenmek için kaybın en aza indirilmesi ve optimize edilmesidir. Gradyanları elde etmek için amaç fonksiyonu türetilmiştir. İki terimden, türev almada toplam kuralını kullanılarak ayrı ayrı türetilmiştir.

Buradaki amaç ise, eğer yanlış sınıflandırılmış bir örnek varsa, ağırlık vektörünü her iki terimin gradyanlarını kullanarak güncellemektir, aksi takdirde doğru sınıflandırılırsa, ağırlık

vektörü sadece düzenleyicinin gradyanı ile güncellenir. Öğrenme oranı, algoritmanın hata eğrisi üzerindeki gradyanı aşağı doğru yaptığı adımların uzunluğudur. Dikkat edilmesi gereken nokta algoritmanın optimal noktayı aşmaması, öğrenme oranının çok olmaması, birleşmenin çok uzun sürmemesidir. Düzenleyici, düşük eğitim hatası elde etme ile sınıflandırıcınızı görünmeyen verilere genelleştirme yeteneği olan düşük test hatası arasındaki dengeyi kontrol etmektedir. Regülasyon parametresi olarak “1/epochs” seçilmiş, bu yüzden epoch sayısı arttıkça bu parametre azalacaktır. Ayrıca düzenleyicinin yüksekliği, düşüklüğü hata olarak değerlendirilir.

#### **3.5.4.4. Rastgele Orman Sınıflandırıcısı ile Sınıflandırma**

RF, karar ağaçları üzerine inşa edilmiş bir sınıflandırıcı olarak nitelendirilebilir. RF’deki her bir ağaç, bir sınıf tahmini oluşturur ve en çok benzerlik alan sınıf, modelinin tahmini olur. Çalışmada öncelikle “estimator” adı verilen tahminçiler ayarlanmıştır ve bu bir diziye atanmıştır. Daha sonra çapraz doğrulama gerçekleştirilmiş ve bunların görselleştirilmesi sağlanmıştır.

Ardından maksimum derinlik ayarı ve minimum örneklerin bölünmesi gerçekleştirilmiştir. Alt kümenin saflık değeri “Gini” rastgele seçildiğinde yanlış sınıflandırılan belirli bir özelliğin olasılık miktarını hesaplamaktadır. Tüm öğeler tek bir sınıfla bağlantılıysa, o zaman saf olarak adlandırılabilir. Gini İndeksi’nin kriteri entropinin özellikleri gibi algıladığında, Gini indeksi “0 ile 1” değerleri arasında değişir, burada “0”, sınıflandırmanın saflığını ifade etmektedir, yani tüm elementler belirli bir sınıfa aittir veya orada sadece bir sınıf vardır. “1”, çeşitli sınıflar arasında öğelerin rastgele dağılımını göstermektedir. Gini İndeksinin 0,5 değeri, bazı sınıflar üzerinde elemanların eşit dağılımını gösterir. Karar ağacı tasarlanırken Gini İndeksinin en düşük değerine sahip olan özellikler tercih edilmiştir. Böylece sınıflandırıcı için çok sayıda parametre uygun değerlerle ayarlanmıştır. Performansın "n\_estimators", "max\_depth" ve diğer parametrelere daha az bağımlı olduğu düşünülmektedir. Modelimizde en iyi parametreler seçilerek sınıflandırmaya verilmiştir.

#### **3.5.4.5. Karar Ağaçları Sınıflandırıcısı ile Sınıflandırma**

DT, sınıflandırma ve regresyon için kullanılan parametrik olmayan denetimli bir öğrenme yöntemi olarak nitelendirilebilir. DT’de amaç, veri özelliklerinden çıkarılan basit karar kurallarını öğrenerek bir hedef değişkenin değerini tahmin eden bir model oluşturmaktır. Sınıflandırmada kullanılan kök düğüm, karar ağacının başladığı yerdir. İki veya daha fazla homojen kümeye ayrılan tüm veri kümesini temsil etmektedir. Yaprak düğümler, son çıktı

düğümüdür ve ağaç, bir yaprak düğüm alındıktan sonra daha fazla ayrılamaz. Bölme ile karar düğümünün/kök düğümün verilen koşullara göre alt düğümlere bölünmesi işlemi gerçekleştirilir. Ağacın bölünmesiyle yeni bir alt ağaç oluşturulur. Budama yapılarak, istenmeyen dalların ağaçtan uzaklaştırılması işlemi gerçekleştirilir. Ağaç ne kadar derin olursa, karar kuralları o kadar karmaşık ve model o kadar uygun olur.

Ağaç oluşturmaya kök düğümle başlanmış ve tüm veri kümesini içeren bir ağaç oluşturulmuştur. Öznitelik seçim kullanarak veri kümesindeki en iyi öznitelik bulunmuş, en iyi nitelikler için olası değerleri içeren alt kümelerle bölünme sağlanarak en iyi özniteliği içeren karar ağacı düğümü oluşturulmuştur. Oluşturulan veri kümesinin alt kümelerini kullanarak yinelemeli olarak yeni karar ağaçları oluşturulmuş; daha sonra sınıflandırmada “max\_depth”, “min\_samples\_split” ve “min\_samples\_leaf” için parametreler ayarlanmıştır. Ardından, çapraz doğrulama için girişler verilmiştir. İnşa edilecek ağaç sayısı tasarlandıktan sonra sınıflandırma modeli oluşturulmuş; sınıflandırma sağlanmıştır.

Bu işlemlerden sonra başarımlarının literatürdeki çalışmalarla kıyaslaması yapılmış ve daha düşük olduğu görülmüştür. Bunun üzerine korelasyon analizi yapmak fikri ile başarımın artabileceği değerlendirilmiştir.

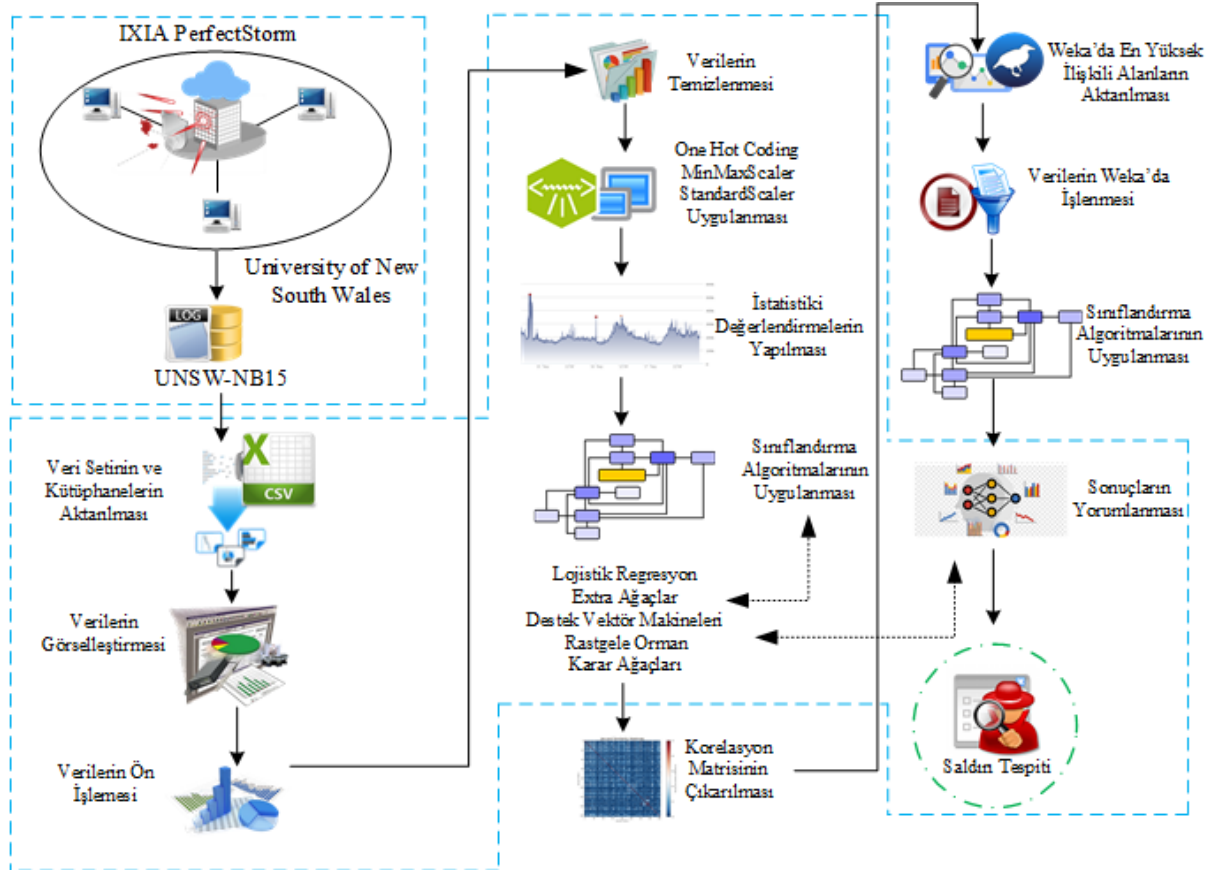
Korelasyon analizi, sayısal olarak ölçülen iki sürekli değişken arasındaki ilişkinin gücünü incelemek için kullanılan bir istatistiksel değerlendirme yöntemi olarak değerlendirilebilir. Bu analiz türü, değişkenler arasında olası bağlantılar olup olmadığını belirlemek amacıyla kullanılır. Çalışmada korelasyon analizi yapılmasının nedeni alanlar arasındaki ilişkilerde sonucu nasıl belirlediği genellikle yanlış anlaşılmaktadır; ancak durum böyle değildir, araştırmada yer almayan diğer değişkenler sonuçları etkilemiş olabilecektir.

Bu amaçla bu analizin yapılması gerekli görülmüştür. İki değişken arasında korelasyon bulunursa, bir değişkende sistematik bir değişiklik olduğunda diğerinde de sistematik bir değişiklik olduğu anlamına gelmektedir; daha sonra değişkenler birlikte değişebilmektedir. Eğer korelasyon bulunursa, ölçülen sayısal değerlere bağlı olarak bu pozitif veya negatif olabilir. Bir değişken diğeriyle aynı anda artıyorsa pozitif korelasyon vardır, yani bir değişkenin yüksek sayısal değerleri diğeri için yüksek sayısal değerleriyle ilişkilidir. Negatif korelasyon, bir değişken azalırken diğeri artarsa vardır, yani bir değişkenin yüksek sayısal değerleri diğeri için düşük sayısal değerleriyle ilişkilidir.

---

*Journal of Management Education* 36(8) 907-924

tüm sembolik ve sayısal olmayan özellikleri kaldırılmıştır. Performansı iyileştirmek için nominal nitelikler sayısal niteliklere dönüştürülmüştür. Bundan sonra, performansı iyileştirmemize ve özelliklerin azaltılmasına yardımcı olan ileriye doğru seçilmiş bir sarmalayıcı seçim yöntemi kullanılmıştır.



Şekil 3.13: Uygulama genel diyagramı

Tüm bu aşamalardan sonra, UNSW-B15 veri kümesinin sınıf değerleri sayısalardan nominale dönüştürülmüştür. Weka veri madenciliği aracı, sayısal değerleri nominal değerlere dönüştürmek için kullanılabilen sayısalardan nominale bir filtreleme sağlanmıştır. Tipik olarak saldırı sınıfı, veri setindeki son öznitelik olarak ele alınmıştır. UNSW-NB15 veri setinin ise 45 numaralı öznitelik olan sınıf değeri ise sayısal değerlerden oluşmaktadır. Weka'da yapılan her deney grubu, gürültüye yanıt olarak ML tabanlı saldırı tespit performansının belirli bir yönünü deneysel olarak test etmeyi amaçlamaktadır. İlk deney grubu, gürültünün potansiyel etkisini ve gürültü filtreleme tekniklerinin ML tabanlı STS'ler üzerindeki etkinliğini araştırmak için ihtiyaç duyulacak olan temel çizginin oluşturulmasını içermektedir. Ayrıca, topluluk öğrenme algoritmalarının kullanımının etkisini ölçmek için kullanılmıştır. Sonraki aşamaların sonuçları,

bu aşamanın sonuçlarıyla karşılaştırılmıştır. İkinci deney setinde, veri setlerine çeyrekler arası gürültü filtreleme algoritması uygulanacaktır.

Bu filtre, veri kümelerinden aykırı değerlerin ve uç değerlerin belirlenmesine yardımcı olacaktır. Bu aşamanın sonuçları temel durum ile karşılaştırılacaktır. Daha sonra, izinsiz giriş veri kümelerine farklı yüzdelere gürültü enjekte edilmiştir. Ardından gürültülü veriler ML'ye eklenecek ilk aşamadan elde edilen temel ile karşılaştırılmıştır. Gürültülü örnekleri hariç tutarak gürültü filtrelemeyi ve ardından, farklı gürültü seviyeleri belirlenmiştir. Bu, aykırı ve aşırı değer örneklerinin olmadığı izinsiz giriş veri kümelerinde çalışan makine öğrenimi algoritmaları üzerindeki gürültünün etkisinin incelenmesine yardımcı olacaktır. Ayrıca, gürültü filtrelemeden önce gürültü enjeksiyonu uygulanmıştır. Bu deneyde, eğitim setinin belirli bir yüzdesinin etiketlerini manipüle etme şeklinde gürültü enjekte edilmektedir. Gürültü filtreleme, uç değerler ve uç değerler kaldırılarak gerçekleştirilmektedir. Son olarak, izinsiz giriş veri kümelerine uygularken, topluluk öğrenme tekniklerini kullanmanın ML algoritmalarının doğruluğu üzerindeki etkisi incelenmiştir.

**Gürültü Enjeksiyonu:** Gürültü, yanlış etiketlenmiş veriler veya yanlış sınıflandırılmış örnekler gibi farklı biçimler alabilir. Daha doğru sonuç elde etmek için, gürültülü veriler önce filtrelenmelidir, çünkü gürültüsüz verilerle çalışmak, fazla uyum gibi olası sorunlardan kaçınmaya yardımcı olmaktadır. Weka'da gürültü, “AddNoise filtresi” aracılığıyla veri kümelerine enjekte edilebilir. AddNoise filtresinde varsayılan gürültü enjeksiyonu değeri %10'dur. Weka'da yapılan çalışmaların ana adımları aşağıdaki gibidir:

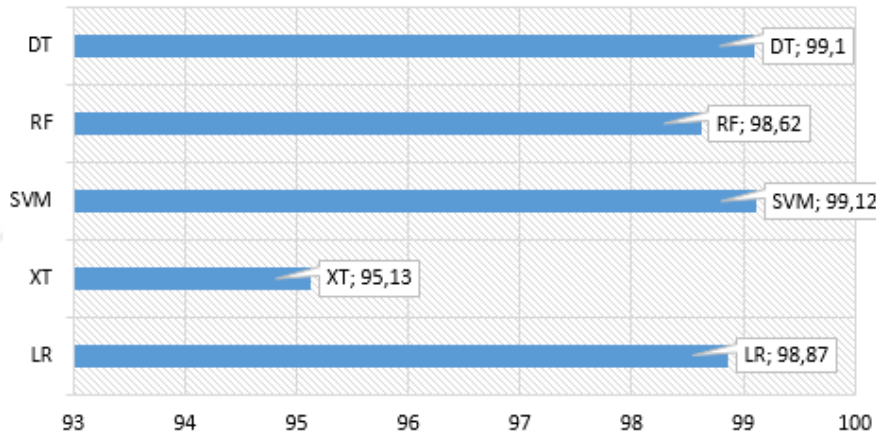
- Eğitim veri setinin yüklenmesi,
- Etiket değerlerini sayısalardan nominale dönüştürülmesi,
- ML algoritmasının eğitim veri kümesinde eğitilmesi,
- Test veri kümesinde ML algoritmasında çalıştırılması,
- Diğer ML algoritmaları kullanarak 3. adıma dönülmesi,
- Eğitim örneklerinin etiketlerini manipüle ederek gürültünün giderilmesi,
- ML algoritmasının gürültülü eğitim veri kümesinde eğitilmesi,
- Test veri kümesinde ML algoritmasının çalıştırılması,
- ML algoritmalarının her biri eğitilip farklı gürültü seviyeleriyle test edilene kadar 3. adıma dönülmesi,
- İzinsiz giriş veri kümesinin eğitim bölümünün yüklenmesi,
- Etiket değerlerinin sayısalardan nominale dönüştürülmesi,

- Aykırı deęerleri ve uę deęerleri kaldırarak gürültü filtrelemesi yapılması,
- ML algoritmasının gürültülü eğitim veri kümesinde eğitilmesi,
- Test veri kümesinde ML algoritmasının çalıştırılması,
- Topluluk öğrenme yönteminin başlatılması (bagging-boosting),
- Temel sınıflandırıcı olarak bir ML algoritması kullanılması,
- Veri kümesinde sınıflandırıcılar topluluğunun eğitilmesi
- Test veri kümesinde sınıflandırıcılar grubunun test edilmesi,
- Her bir ML algoritması her iki topluluk öğrenme yöntemiyle de kullanılabileceğine kadar adımların tekrarlanması.

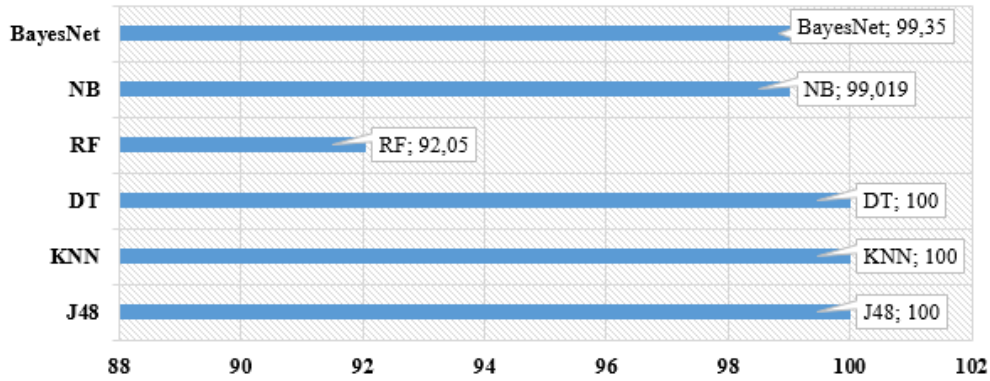
Şekil 3.13'te uygulamaya dair tüm adımlar genel diyagram şeklinde verilmiştir. Çalışma temel yapı olarak ikiye ayrılmaktadır. İlk adım Google Colab üzerinde gerçekleştirilmiş olup daha sonra ise Weka'da bir takım deneysel çalışmalar gerçekleştirilmiştir. Weka'daki uygulamalar temel olarak kendi içinde ikiye ayrılmaktadır. İlk adım tüm veri setinde çalışmalar yapılması; ikinci adım ise Colab ile ön işlenmiş verinin alınıp yukarıdaki adımlarla tekrar analize edilmesidir. Yapılan tüm bu deneysel çalışmalara ve uygulamalara ait sonuçlara 4. bölümde yer verilmiştir.

#### 4. BULGULAR

Log dosyaları, ağ üzerinde denetimi sağlamak için en önemli veri kaynağıdır. Bu sebeple log dosyası olarak gerçek hayattaki modern senaryoların yanı sıra ağ trafiğinden elde edilen verilerden ve çeşitli saldırı aktivitelerinden oluşan “UNSW\_NB15 Dataset” kullanılmıştır. Söz konusu veri seti normal ve anormal ağ etkinliklerini barındırmaktadır. Veri setindeki toplam örnek sayısı 2.540.044’tür. Çalışmada veri kümesinin eğitim ve test veri kümelerinden oluşan ve 257.673 örnek içeren bir alt kümesi kullanılmıştır. Eğitim seti 175.341 örnek, test seti ise 82.332 örnek içermekte olup “Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode ve Worms” saldırılarını ve normal aktiviteleri içermektedir. Gerçekleştirilen uygulamayı çalıştırmak için kullanılan ortam, Tesla K80 GPU kullanılan ücretsiz Google Colab sürümü kullanılmıştır.



Şekil 4.1: Colab uygulaması sınıflandırma başarımları



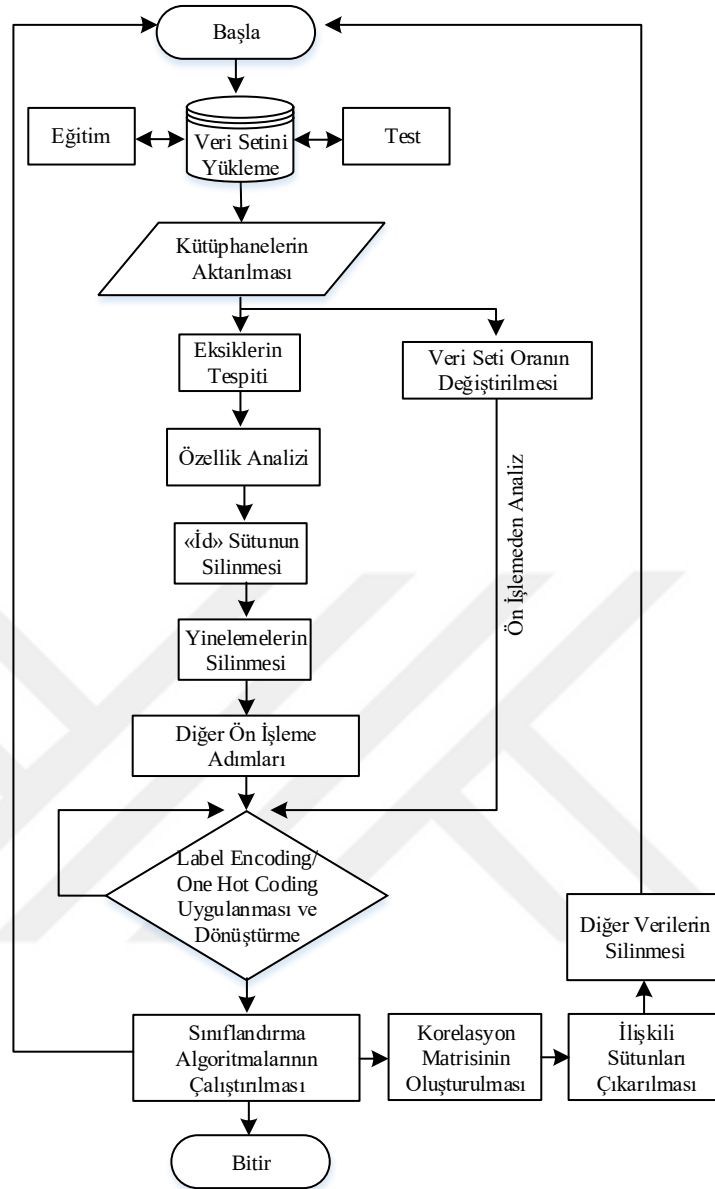
Şekil 4.2: Weka analizi sınıflandırma başarımları

Şekil 4.1’de Colab üzerinde yapılan uygulama ile elde edilen başarımların oranlarına yer verilmiştir. Şekil 4.2’de ise Weka üzerinde yapılan uygulama ve deneyler sonucunda elde edilen çalışmalara ait başarımların oranlarına yer verilmiştir.

**Tablo 4.1:** Uygulamaların genel sonuçları

| COLAB UYGULAMA SONUÇLARI |               | WEKA UYGULAMA SONUÇLARI |               |
|--------------------------|---------------|-------------------------|---------------|
| ALGORİTMA                | BAŞARIM ORANI | ALGORİTMA               | BAŞARIM ORANI |
| RF                       | 98,62%        | RF                      | 92,05%        |
| DT                       | 99,10%        | DT                      | 100%          |
| LR                       | 98,87%        | KNN                     | 100%          |
| XT                       | 95,13%        | NB                      | 99,19%        |
| SVM                      | 99,12%        | BayesNet                | 99,35%        |

Tabl 4.1’de uygulamaların toplu olarak verilen test sonuçlarından görüldüğü gibi, Weka ile yapılan işlemlerde RF %92,05 ile en düşük başarımlar oranını vermiştir. DT, J45 ve KNN yöntemlerini kullanarak Weka ile analiz sonucunda en yüksek başarımlar elde edilmiştir. Colab uygulamasında en yüksek başarımlar DT yöntemi ile elde edilmiştir. Colab uygulamasında en düşük başarımlar XT yönteminin uygulaması ile gerçekleştirilmiştir. SVM Colab uygulamasında diğerleri ile karşılaştırıldığında daha yüksek bir doğruluk puanı üretmiştir. PyCaret kütüphanesi, bu araştırmanın kısa sürede ve geldiğinde daha az güçlüklerle yapılmasını sağlamıştır. PyCaret’in ayarlama fonksiyonu da çalışmaya katkıda bulunmuştur.



Şekil 4.3: Uygulanan akış şeması

UNSW-NB15 veri kümesinin saldırılarının, bazılarının 0'a yaklaşma olasılığı ile ciddi şekilde dengesiz olduğu tespit edilmiştir. Bu, veri kümesinin yalnızca %2,08'ini temsil eden Analiz, Arka Kapı, Kabuk Kodu ve Solucanlar gibi olası en düşük saldırı sınıflarının sınıflandırma doğruluğunu olumsuz etkilemektedir. Bu arada, bu saldırı sınıfları veri kümesinin %68'inden fazlasını temsil ettiğinden, Exploits ve Generic sınıflarında önemli ölçüde yüksek bir performans elde edilebilmektedir. Önerilen model, Weka'da yalnızca RF hariç önemli ölçüde daha iyi performans göstermiştir. Makine öğrenimi tespit ve sınıflandırma aşamaları birleştirildiğinde, genel performans önemli ölçüde bozulmuştur.

Bu çalışma, ilgili özellikleri ve yaygın siber güvenlik açıklarını içeren gerçeğe en yakın ağ trafiği veri setini kullanan ağ saldırı tespit sistemlerini ele almıştır. Yarı dinamik hiper parametre ayarlama yaklaşımıyla birleştirilmiş önerilen derin öğrenme sınıflandırma mimarisi, benzer derin öğrenme tabanlı ağ STS'lerinin sonuçlarına kıyasla çok sınıflı modellerde önemli gelişmeler göstermiştir. Her veri kümesi için en iyi performansa sahip ML algoritmasını belirlemek için birçok deney yapılmıştır. Ayrıca, eğitim setinin performans metrikleri sonuçları: doğruluk, kesinlik, hatırlama, f1-skor, ROC ve CM test sonuçlarından daha yüksek olduğu ve başarımları ile aynı sıralamada olduğu tespit edilmiştir. Genel olarak, modeller 'normal' verileri doğru bir şekilde tahmin ederken, izinsiz girişleri tahmin ederken yanlış sınıflandırmaların meydana geldiği görülmektedir.

Özellik seçimi için birliktelik kuralına dayalı bir teknik uygulanmıştır. Her özellik için nokta model seçimi kullanılmıştır. Sık değeri belirlemek için işlem süresi azaltılmış ve alakasız veya gürültülü özellikleri kaldırarak en yüksek sıradaki özellikler bulunmuştur. Bu işlemlerin sonucunda, makine öğrenimi modelinin girdisi oluşturulmuştur. Bu durumda yanlış negatif ile ilişkili maliyet çok düşük olmalıdır. Weka'da gerçekleştirilen deneysel çalışmalar:

- Etiket değerlerini sayısalardan nominale dönüştürülmesi,
- Eğitim örneklerinin etiketlerini manipüle ederek gürültünün giderilmesi,
- ML algoritmasının gürültülü eğitim veri kümesinde eğitilmesi,
- ML algoritmalarının her biri eğitilip farklı gürültü seviyeleriyle test edilene kadar adım tekrarı,
- Aykırı değerleri ve uç değerleri kaldırarak gürültü filtrelemesi yapılması,
- ML algoritmasının gürültülü eğitim veri kümesinde eğitilmesi,
- Topluluk öğrenme yönteminin başlatılması (bagging-boosting),
- Temel sınıflandırıcı olarak bir ML algoritması kullanılması,

şeklinde. Bu temel adımlarla başarımları artmıştır. Sadece verilerin yüklenmesi ve sınıflandırması ile başarımlarının çok daha düşük olduğu gözlemlenmiştir.

Colab'da ise ön işlemleri gerçekleştirilmeden sadece veri setinin normal dağılımı ile başarımların çok daha düşük olduğu sonucu çıkarılmıştır. Örneğin ön işleme olmadan LR'de %81,78 başarımları onarına ulaşılmıştır.

```

▶ logisticR=SGDClassifier(alpha=lr_cfl.best_params_['alpha'],
eta0=lr_cfl.best_params_['eta0'], penalty='l2',
loss='log', n_jobs = -1, max_iter=lr_cfl.best_params_['max_iter'])
logisticR.fit(df_train,y_train)
sig_clf = CalibratedClassifierCV(logisticR, method="sigmoid")
sig_clf.fit(df_train, y_train)
predict_y_tr_lr = sig_clf.predict(df_train)
predict_y_te_lr = sig_clf.predict(df_test)
lr_f1 = f1_score(y_test, predict_y_te_lr)
print(lr_f1)

```

0.8178902770626124

**Şekil 4.4:** Ön işlemez sınıflandırma sonucu (LR)

Şekil 4.4'te ön işleme yapılmadan önce LR sınıflandırıcısı ile yapılan sınıflandırmanın sonucu ve temel kod yapısına yer verilmiştir. Bu sonuca bakıldığı zaman veri ön işleme, model oluşturma için makine öğreniminde ilk ve en önemli adım olduğu gerçeği bir kez daha görülmüştür. Sistem tarafından toplanan veriler genellikle tutarsızdır, ön işleme ile verileri görselleştirme ve analiz adımı hazırlamaktadır. Her bir özellik incelenmiş, veriler çarpık olduğu için görselleştirmeden önce normalleştirilmesi gerekli olmuştur. İlk olarak, bu öznitelikteki benzersiz numaralandırma nedeniyle mükerrer kayıtlar tanımlanamadığından, "id" özneliği her iki veri kümesinden de çıkarılmıştır. Bu ve benzeri temizleme işlemlerinin de ne kadar önemli olduğu ortaya çıkmıştır. Daha sonra veri kümelerindeki hem eğitim hem de test veri kümelerinden yinelenen işlemlerle önemli veriler bulunmuş ve çıkarılmıştır. Hem Colab'da hem de Weka'da veri setindeki oranlar değiştirilmiş, eğitim veri seti ile test veri seti yer değiştirilmiş ve test veri setinin sınıflandırmada daha iyi sonuçlar verdiği gözlemlenmiştir.

Kodlanmış değişkenler ve çıkarılan özellikler incelenmiş; yalnızca veri kümesinin boyutsallığını artırmış olduğu için öncelikle özellikler arasında korelasyon çıkarmıştır. Veri analizi adımı geçmeden önce, özelliklerin nasıl dağıtıldığını daha iyi anlayabilmemiz için veri kümesinden aykırı değerlerin kaldırılması sağlanmıştır.

## 5. TARTIŞMA

Siber tehditlerin ve saldırıların sürekli artması nedeniyle STS yeteneklerinin optimize edilmesi önemli bir gereklilik haline gelmektedir. ML tabanlı STS'ler, kötüye kullanım ve anormallik saldırılarına karşı koymak için kullanılabilecek yeni ortaya çıkan paradigmalardan olmaktadır. Bununla birlikte, ML tabanlı STS'lerin sınıflandırma doğruluğu birkaç faktöre bağlıdır. Bu faktörlerin belirlenmesi, daha iyi ML tabanlı STS'ler oluşturmaya yardımcı olmaktadır. Bu çalışmanın deneylerinden elde edilen sonuçlar, ML tabanlı sınıflandırma doğruluğunun STS'lere ait belirli faktörlerden etkilenebildiğini açıkça ortaya koymuştur.

Bu faktörler, eğitim ve test için veri setini kullanma yöntemi, aykırı değerlerin ve uç değer örneklerinin kaldırılması, yanlış etiketlenmiş örneklerin eklenmesi, ön işlemenin sağlıklı gerçekleştirilmesi, deneysel çalışmaların fazlalığı, uygun yöntem gerçekleştirilmesi ve topluluk öğrenme tekniklerinin kullanılmasıdır. Bu faktörlerin sınıflandırma doğruluğu üzerinde birçok etkisi vardır. Bazı durumlarda, gürültünün doğruluk üzerindeki olumlu etkisi olduğu gibi, bu faktörler çoğu zaman da sınıflandırma doğruluğu üzerinde olumsuz bir etkiye neden olmaktadır. Öte yandan, bu faktörlerin bazıları, UNSW-NB15 veri kümesine uygulandığında bazı sınıflandırma algoritmalarının başarımının artmasında büyük bir iyileşmeye neden olmuştur ve bazı durumlarda da bu faktörler ML tabanlı doğrulamanın doğruluğunu etkilememiştir. Tablo 5.1'de çalışmamız ile örtüşen en güncel kaynaklara ait bazı bilgilere yerilmiştir. Tablo 5.1'de çalışmamız ile örtüşen en güncel kaynaklarla başarımların kıyaslamamız sunulmuştur.

**Tablo 5.1:** Çalışmaya benzer en güncel kaynaklar

| K.N  | KULLANILAN YÖNTEM                                                                      | YIL  | VERİ SETİ                     | GELİŞTİRME ORTAMI                   |
|------|----------------------------------------------------------------------------------------|------|-------------------------------|-------------------------------------|
| [24] | KNN, RF, LR, NB, DT, Gradient Boosting Classifier, Adaptive Boot Classifier, Blending. | 2021 | UNSW-NB15                     | Google Colaboratory-PyCaret Library |
| [39] | DT, RF, SVM, NB, ANN                                                                   | 2021 | KDD'99, UNSW-NB15             | Weka                                |
| [41] | SVM, NB, DNN                                                                           | 2021 | UNSW NB15                     | Google Colab                        |
| [50] | DNN                                                                                    | 2021 | UNSW NB15                     | Google Colab (Keras, TensorFlow)    |
| [56] | RF, J48, NB, SVM, Bayesian Network, Bagging, AdaBoost                                  | 2021 | KDD99, UNSW-NB15, CIC-IDS2017 | Weka                                |

**Tablo 5.2:** Benzer çalışmalarla başarımların karşılaştırması

| S.N.                     | KNN   | RF    | LR    | NB    | DT    | SVM   | J48   | BAYESNET |
|--------------------------|-------|-------|-------|-------|-------|-------|-------|----------|
| [69]                     | 86,46 | 87,22 | 83,56 | 73,86 | 86,37 | X     | X     | X        |
| [84]                     | X     | 96,34 | X     | 91,55 | 100   | 100   | X     | X        |
| [86]                     | X     | X     | X     | 92,16 | X     | 92,13 | X     | X        |
| [101]                    | X     | 98,30 | X     | 96,13 | X     | X     | 97,40 | 96,23    |
| Gerçekleştirilen Çalışma | 100   | 95,33 | 98,87 | 99,19 | 99,55 | 99,12 | 100   | 99,35    |

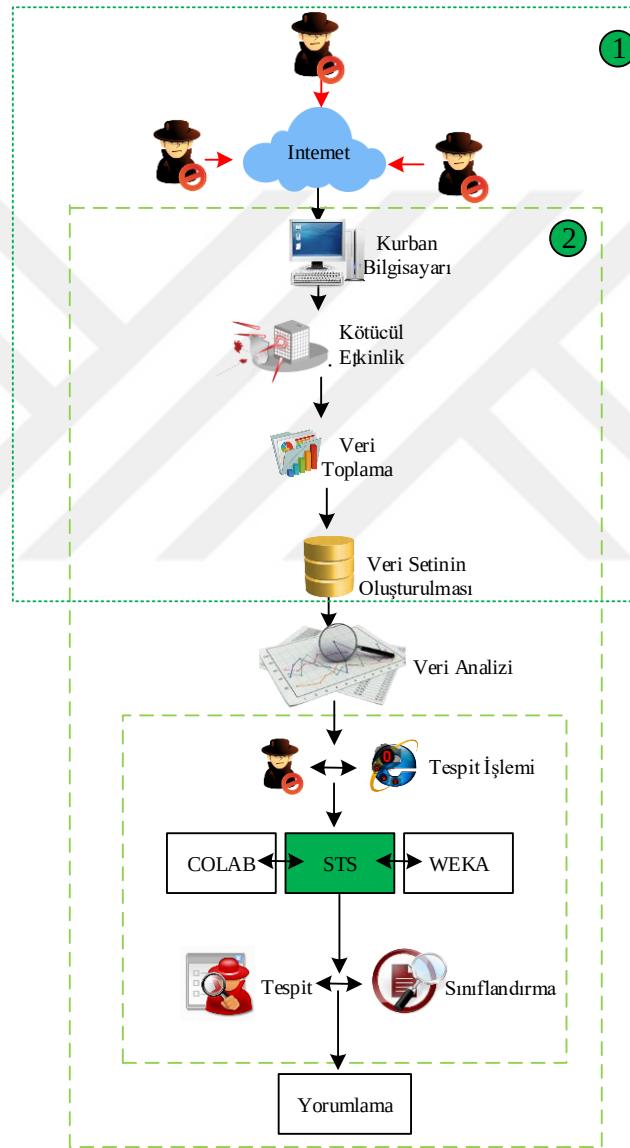
Iqbal ve diğ. (2021) çalışmalarında, PyCaret makine öğrenimi kitaplığını kullanarak ve genel performansını analiz ederek IoT ağlarındaki botnetleri tespit etmek için daha verimli bir makine öğrenimi yaklaşımı amaçlanmıştır. PyCaret makine öğrenimi kitaplığını kullanarak ve genel performansını analiz ederek IoT ağlarında botnet'leri algılamak için daha verimli bir makine öğrenimi yaklaşımı belirlemeyi amaçlanmıştır. Yapılan araştırma, farklı sınıflandırıcıları kapsayacak ve her biri için farklı performans ölçütlerini analiz edecek şekilde gerçekleştirilmiştir. Ayrıca PyCaret kütüphanesini kullanmanın gerekliliği ve bu kullanım için ne kadar uygun olduğu konuları ele alınmıştır [69].

Al-Gethami ve diğ. (2021) çalışmalarında, DT, RF, SVM, ANN ve NB kullanılarak ML tabanlı STS'lerin sınıflandırma doğruluğunun belirli faktörlerden etkilenebileceğini göstermek amaçlanmıştır. Çalışmada ele alınan faktörler, eğitim ve test için veri setini kullanma yöntemi, aykırı değerlerin ve uç değer örneklerinin kaldırılması, yanlış etiketlenmiş örneklerin eklenmesi ve topluluk öğrenme tekniklerinin kullanılmasıdır. Bu faktörlerin sınıflandırma doğruluğu üzerinde çeşitli etkileri gösterilmiş; bazı durumlarda, verilerde oluşan gürültünün RF algoritmasının doğruluğu üzerindeki etkisi, sınıflandırma doğruluğu üzerinde olumsuz etkileri gösterilmiştir. Bu faktörlerin olumsuz etkilerinin, UNSW-NB15 veri kümesine uygulandığında DT, RF, SVM, ANN ve NB algoritması gibi sınıflandırma yöntemleriyle büyük bir iyileşme sağladığı gösterilmiştir [84].

El-Sayed ve diğ. (2021) çalışmalarında, akıllı taşıma sistemlerinde saldırı tespitine yönelik bir öneri sunulmuştur. Bu öneri için veri setindeki yalnızca 20 özellik kullanılmıştır. Yöntem olarak SVM, ANN ve NB algoritmaları kullanılmış, önerilen yöntem ile doğruluk değerinin arttığı tespit edilmiştir [86].

Acharya ve diğ. (2021) çalışmalarında, Weka kullanılarak KDD99, UNSW-NB15 ve CIC-IDS2017 ağ günlükleri trafiğini kullanan veri setleri üzerinde RF, J48, NB, BayesNet, Bagging,

AdaBoost ve SVM dâhil olmak üzere çeşitli makine öğrenimi algoritmalarının etkinliği tartışılmıştır. Ağ saldırı veri kümelerinin çıktı sınıflarının sayısının değiştirilmesinin duyarlılık, TPR, FPR, AUC ve yanlış tanımlanan yüzde üzerindeki etkisini incelemişlerdir. Hedef sınıf sayısı azaldığında makine öğrenimi sınıflandırıcılarının performansının arttığı ve çıktı sınıfına yüksek düzeyde ilişkili bir özelliğin eklenmesiyle, sınıflandırıcıların performansının arttığı ortaya konulmuştur [101].



**Şekil 5.1:** İncelenen sistemin kavramsal çerçevesi

Bu tez çalışmasında ise ilk olarak veri temizleme için analizler, her bir özelliğin açıklaması incelenmiş, veriler çarpık olduğu için görselleştirmeden önce normalleştirilmesi sağlanmıştır. Mükerrer kayıtlar çıkarılmış, daha sonra veri setindeki saldırı tiplerini içeren öznitelik ikili

sınıflandırma problemlerinde gereksiz olduğu için kaldırılmıştır. Veri kümesinde eksik olan değerlerle başa çıkmak için, PyCaret varsayılan olarak sayısal özellikler durumunda özelliğin ortalama değerini kullanmaktadır. Medyan değerinin standart değer ile daha uygun sonuç verdiği gözlemlenmiş, normalleştirme ve dönüşüm işlemleri gerçekleştirilmiştir. Veri setinde ilişkiler gözlemlemek adına veriler görselleştirilmiş, apriori algoritması kullanılarak birliktelik kuralı oluşturulmuş, güven ve artış sırasına göre sıralama yapılmıştır. Şekil 5.1’de kavramsal çerçeveye yer verilmiştir. Şekilde görülen yapıda 1. alan Avustralya’daki “University of New South Wales”de IXIA PerfectStorm aracı tarafından hazırlanmış normal ve anormal ağ etkinliklerini barındırmaktadır.

Bir takım küçük adımlardan sonra veri setinin alanlarından nominal olan alanların her biri “One Hot Encoding” kodlama yöntemi kullanılmıştır. Daha sonra aynı işlemi test verilerine uygulayabilmemiz için tüm önemli parametreler ve nesneler diske kaydedilmiştir. Özellik ölçeklendirme işlemi gerçekleştirilmiştir. Daha sonra LR, XT, SVM, RF ve DT yöntemleri ile sınıflandırmalar gerçekleştirilmiştir. Daha sonra hem ön işlenmiş verilerle hem de tüm veri seti birleştirilerek çapraz doğrulama yöntemi adı verilen “Cross Validation” ile KNN, BayesNet, NB, DT ve RF algoritmaları ile tekrar analizler ve deneyler yapılmıştır. Tüm bu deneylerin sonucu Tablo 5.1’de verilen çalışmaların sınıflandırma yöntemlerine göre başarımlarını içeren Tablo 5.2’de sunulmuştur.

## 6. SONUÇ VE ÖNERİLER

Bilgi ve bilgi sistemleri güvenliğinin öneminin hızla gelişen teknoloji ile birlikte artması, sistem güvenliği konularında alınması gereken tedbirlerin gerekliliğini de en üst düzeye çıkartmıştır. Bilgi güvenliği sistemlerinde kullanılan araçlar çok çeşitli ve güçlü olsa da, gelişen yeni teknolojilerden kaynaklanan yeni güvenlik açıklıklarını bulma noktasında başarılı olamayabilmektedir ve bu sebeple hiçbir zaman yüzde yüz güvenli bir sistemden söz edilememektedir. Kötücül girişimlerden önce saldırganların nasıl saldırabileceğini tespit etmek ve buna göre güvenliği sağlamak, alınan tedbirlerin etkisini en yüksek seviyeye çıkaracaktır.

Kritik altyapı sistemleri, gelişen teknoloji ile birlikte modern toplumların temelini oluşturmaktadır ve ulusal refahın korunması için önem arz etmektedir. Genellikle tarım, su, elektrik şebekesi, ulaşım, iletişim ve teknoloji sistemleri ile çeşitli kamu ve özel sektör yapılarını içeren bu sektörler günlük hayatın devamını sağlamak için son derecede elzemdir. Birbirine bağlı ve bağımlı hale gelen karmaşık sistemler olan bu yapıların sadece bir parçasının arızalanması bile diğer bağımlı sistemlerin arızalanmasına neden olmakta ve arızanın meydana geldiği altyapıyı tümüyle etkileyebilmektedir. Ayrıca, devletlerin güvenliği, ekonomisi ve ayrıca vatandaşların refahı için önemli birer etken olarak karşımıza çıkmaktadır. Bu nedenler göz önüne alındığında kritik altyapıların güvenliğinin sağlanması siber güvenlik çatısı altında hayati bir rol taşımaktadır ve bu tür altyapıların güvenliğinin Türkiye'de tam olarak sağlanması hususuna önem verilmelidir. Kritik altyapı korumasına ilişkin sorunlar, siber güvenlik konusundaki çalışmaların gölgesinde kalmaya devam etmemelidir ve gerekli tüm çalışma ve işbirliklerinin de yapılması gerekmektedir.

Siber güvenlik, siber saldırılara karşı alınması gereken önlemler bütünü olarak değerlendirilmelidir. Ayrıca kurum, kuruluş ve kullanıcıların varlıklarını korumak için araçlar, politikalar ve uygulamalar geliştirmeli; hukuki belgeler, elektronik medya belgeleri, etkinlikler, eğitimler ve güvenlik teknolojileri, ulusal/uluslararası işbirliği düzenlemelidir. Kritik altyapı, teknoloji gelişimi ve siber uzayın büyümesiyle bu alanda eğitim alanında da çalışma yapılmasını zorunlu kılmıştır. Bu zorunlulukla farkındalık eğitimler, seminerler, konferanslar düzenlenmeli, müfredatlara bu konularda dersler eklenmelidir. Bu alanda çalışacak uzman ekip yetiştirilmesi için önemli bir adım olan yazılım eğitimi, bilgisayar mühendisliği bölümlerinde yazılım derslerinin verilmesi, yazılıma dair kurslar verilmesi şeklinde de gerçekleşmektedir. Ancak mühendislik belirli bir konuya bütüncül yaklaşımdır, bu anlamda ülkemizde yazılım öğrenmede diğer yöntem ise yazılım mühendisliği bölümüdür. Yazılım mühendisliğinde dersler

çok daha uygulamaya yöneliktir ve sistemden ziyade yazılım konularına ağırlık verilmektedir. Yazılım mühendisliğini ayıran bir diğer konu da derslerin uygulama temelli olarak yazılım analizi, tasarımı, proje yönetimi, proje testi, işyeri eğitimi gibi farklılıklara sahip olmasıdır.

Son yıllarda bilgi güvenliğine yönelik tehditler, dünyada aktif olarak kullanılan hizmetlere yönelik istismarların ve tehditlerin şirketler için bir kâr modeli haline gelmesi nedeniyle daha hedef odaklı bir hale gelmiştir. İstismarlar ve taviz verme teknikleri daha karmaşık ve detaylı hale gelirken, günlük erişim kayıtlarının analizi ile tehdit izleme, bilgi güvenliğinin önemli bir faktörü haline gelmiştir. SIEM, ağ ve güvenlik cihazlarından veri toplama ve analiz etme yeteneklerine sahiptir. SIEM, günümüzde birçok siber güvenlik operasyon merkezinin kullandığı izleme yeteneklerini geliştirmek için çeşitli güvenlik cihazlarından gelen olayları ilişkilendirmek için tüm önemli bilgileri birleştirilmiş bir çerçevede toplamak için kullanılan bir yöntemdir. SIEM, ağ cihazlarından, sunuculardan, etki alanı denetleyicilerinden ve daha fazlasından güvenlik verilerini toplamaktadır; verilerdeki eğilimleri, tehditleri tespit etmek ve kullanıcıların uyarıları araştırmasını sağlamak için bu verileri depolayıp normalleştirmekte ve bu verilere analitik yöntemler uygulamaktadır. SIEM, bir olay müdahale ekibine güvenlik olayları hakkında raporlama imkânı veren ve belirli bir kural kümesiyle eşleşen ve bir güvenlik sorununu uyarılarla belirten, veri toplayıcı, izleyici ve raporlama sistemidir. SIEM temelde bilgi güvenliğinin üç ana kavramının sağlanmasına yönelik çalışmaktadır. Siber güvenlik ortamının ne kadar hızlı değiştiği göz önüne alındığında, kuruluşların hem bilinen hem de bilinmeyen güvenlik tehditlerini algılayabilen ve bunlara yanıt verebilen çözümlere güvenilebilmesi gerekmekte; bu noktada SIEM ürünleri kullanmak veya kendi yazılımını kurumun kendisinin geliştirmesi gerekecektir.

Bu tez çalışmasında, öncelikle kritik altyapı tanımına ve detaylarına yer verilmiş; bu yapıların korunmasına yönelik önlem alınması aşamasında bir farkındalık oluşturmak amaçlanmıştır. Daha sonra ülkelerin siber güvenlik politikaları bir ilişkiyel yapıda verilmiş gerçekleştirilen çalışmalar ve politikalar birçok kapsamda değerlendirilmiştir. Türkiye'nin siber güvenlik alanındaki politikalarını bu anlamda geliştirilen çalışmalara ve hukuksal çalışmalarına yer verilmiştir. Ayrıca bir bütün olarak da değerlendirilebilen kritik altyapı SIEM ilişkisinin ve teknolojik gelişmelerin bir zorunluluğu sonucu olarak yazılım mühendisliği kavramı ele alınmış; ulusal ve uluslararası anlamda yazılım mühendisliği hakkında bilgiler verilmiştir. Gerçekleştirilen tez çalışmasında son zamanlarda kritik altyapı, siber güvenlik politikaları ve SIEM'i içeren güncel çalışmalar araştırılmış ve akademik ve idari çalışmalar kapsamlı bir şekilde yer verilmiştir. Tez çalışmasının uygulama bölümünde ise gerçek hayattaki modern

normal senaryoların yanı sıra ağ trafiğinden elde edilen verilerden ve çeşitli saldırı aktivitelerinden oluşan “UNSW\_NB15 Dataset” i üzerinden uygulama geliştirilmiştir.

Geliştirilen uygulama ile “Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode ve Worms” olmak üzere dokuz tür saldırı ve Normal aktivitelerden oluşan kategori ile toplamda 10 kategori altında analiz gerçekleştirilmiştir. Çalışma temel yapı olarak ikiye ayrılmaktadır. İlk adım Colab üzerinde gerçekleştirilmiş olup daha sonra ise Weka’da bir takım deneysel çalışmalar gerçekleştirilmiştir. Weka’daki uygulamalar temel olarak kendi içinde ikiye ayrılmaktadır. İlk adım tüm veri setinde çalışmalar yapılması; ikinci adım ise Colab ile ön işlenmiş verinin alınıp yukarıdaki adımlarla tekrar analize verilmesidir. Yapılan tüm bu deneysel çalışmalara ve uygulamalara ait sonuçlara 4. bölümde yer verilmiştir.

İlk olarak veri temizleme için analizler, her bir özelliğin açıklaması incelenmiş, veriler çarpık olduğu için görselleştirmeden önce normalleştirilmesi sağlanmıştır. Mükerrer kayıtlar çıkarılmış, daha sonra veri setindeki saldırı tiplerini içeren öznitelik ikili sınıflandırma problemlerinde gereksiz olduğu için kaldırılmıştır. Veri kümesinde eksik olan değerlerle başa çıkmak için, PyCaret varsayılan olarak sayısal özellikler durumunda özelliğin ortalama değerini kullanmaktadır. Medyan değerinin standart değer ile daha uygun sonuç verdiği gözlemlenmiştir. Normalleştirme ve dönüşüm işlemleri gerçekleştirilmiştir. Veri setinde ilişkiler gözlemlenmek adına veriler görselleştirilmiş, apriori algoritması kullanılarak birliktelik kuralı oluşturulmuş, güven ve artış sırasına göre sıralama yapılmıştır.

Bir takım adımlardan sonra veri setinin alanlarından nominal olan alanların her biri “One Hot Encoding” kodlama yöntemi kullanılmıştır. Daha sonra aynı işlemi test verilerine uygulayabilmek için tüm önemli parametreler ve nesneler diske kaydedilmiştir. Özellik ölçeklendirme işlemi gerçekleştirilmiştir. Daha sonra LR, XT, SVM, RF ve DT yöntemleri ile sınıflandırmalar gerçekleştirilmiştir. Daha sonra hem ön işlenmiş verilerle hem de tüm veri seti birleştirilerek çapraz doğrulama yöntemi adı verilen “Cross Validation” ile KNN, BayesNet, NB, DT ve RF algoritmaları ile tekrar analizler ve deneyler yapılmıştır. Tüm bu deneylerin sonucunda Colab ile geliştirilen uygulamada RF’de %98,62, DT’de %99,10, LR’de 98,87, XT’de 95,13 ve SVM’de %99,12 başarımlar elde edilmiştir. Daha sonra Weka’da yapılan çalışmalar ve deneyler sonucunda RF’de %92,05, DT’de %100, KNN’de %100, J48’de %100, NB’de %99,19 ve BayesNet’de %99,35 başarımlar elde edilmiştir.

Tüm bu adımlar ve çalışmalardan yola çıkarak devletler, kurumlar, kuruluşlar ve kullanıcıların varlıklarını korumak için araçlar, politikalar ve uygulamalar geliştirmelidir. Hukuki belgeler, elektronik medya belgeleri, etkinlikler, eğitimler ve güvenlik teknolojileri,

ulusal/uluslararası işbirliği düzenlemeleri önemli bir husus olarak değerlendirilmektedir. Bilgi teknolojilerindeki gelişmeler hem altyapıları hem de altyapılar arasındaki ilişkileri ve bağımlılığı etkilediği için bu sistemlerin fiziksel güvenlik yanında mantıksal güvenliği de ön plana çıkmıştır. Çünkü günümüzde kritik altyapı BT (Bilgi Teknolojileri) sistemleri genellikle bilgisayar sistemleri ile kontrol edilmekte ve izlenmektedir. Bilgisayar sistemleri de TCP/IP protokol ailesini kullandığı için internete bağlı olsa da olmasa da güvenlik riskleriyle karşı karşıyadır. İlerleyen çalışmalarda Colab üzerinde yapılan çalışmanın anlık veri analizi ve saldırı tespiti yapacak bir sistem olarak geliştirilmesi planlanmaktadır. Bu sistemin yoğun raporlama ve grafiklendirme altyapısının olması operasyon personel için faydalı olacaktır. Ayrıca kurulacak bir sistem ile veri setlerinin tarafımızca tutulması daha gerçekçi analiz ve geliştirme sağlamak adına faydalı olacaktır. Gerçekleştirilecek çalışmada ayrıca anlık olarak sistemde paket analizi ve şüpheli paket tespiti yapılması ve SIEM mantığından hareketle tutulan logların ve farklı türlerdeki mevcut log dosyalarının analizinin gerçekleştirilmesi planlanmaktadır. Bu analiz sınıflandırma algoritmaları gibi yöntemlerin dışında daha güncel teknolojiler kullanılarak gerçekleştirilecektir.

## KAYNAKLAR

- [1]. Karaca, M. ve Gül, E., 2021, *Kritik altyapılara yönelik bilişim suçları, Türkiye ve AB uygulamaları*, Bilişim Hukuku Dergisi, 3(1), 1-30.
- [2]. Kışman, Z.A., ve Güleç, Ö., 2021, *Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri*, Akademik Açı, 1(1), 127-154.
- [3]. Karabacak, B., Yildirim, S. O. ve Baykal, N., 2016, *Regulatory approaches for cyber security of critical infrastructures: the case of Türkiye*, Computer law & security review, 32(3), 526-539.
- [4]. Demir, Ü., 2021, *Uluslararası Güvenlik Açısından Ülkemizdeki Bilgi Güvenliği ve Siber Güvenlik Eğitimlerinin Mevcut Durumunun İncelenmesi*, İRÜİSTANBUL, 2-7.
- [5]. Köker, A.E., 2021, *Ulusal Siber Güvenlik Stratejisi: Fransa*, UPA Strategic Affairs, 3(1), 42-78.
- [6]. Ünal, S., 2021, *Siber uzama yönelik politik söylemde iletişim güvenlik yakınsaması: ABD, AB ve Türkiye örneği*, Akademik Hassasiyetler, 8(17), 369-399.
- [7]. Eldem, T., 2021, *Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik*, İstanbul Hukuk Mecmuası, 79(1), 345-376.
- [8]. Akdağ, İ., 2021, *Siber güvenlik ve Türkiye, örgütsel yapı, uygulamalar ve gelecek*, Tez (Doktora), Hacettepe Üniversitesi
- [9]. Tuğal, İ., Almaz, C., ve Sevi, M., 2021, *Üniversitelerdeki siber güvenlik sorunları ve farkındalık eğitimleri*, Bilişim Teknolojileri Dergisi, 14(3), 229-238.
- [10]. Çıtak, E., 2021, *Siber terörizm: potansiyelin gerçekçi tehdidi*, Turkuaz Uluslararası Sosyo-Ekonomik Stratejik Araştırmalar Dergisi, 3(4), 1-16.
- [11]. Küçük, M., 2021, *Avrupa Birliği'nin güvenlik strateji belgelerinin analizi*, Diplomasi Araştırmaları Dergisi, 3(1), 37-49.
- [12]. Karasoy, H.A., 2021, *Değişen kamu güvenliği anlayışı ve yeni nesil savaş*, ASSAM Uluslararası Hakemli Dergi, 8(19), 56-70.
- [13]. Şeşen, Y. ve Kuzucuoğlu, A.H., 2021, *Intelligence Activities In The Context Of Data And Information Security*, Library Archive and Museum Research Journal, 3(1), 36-56.
- [14]. Ocak, H.S., 2021, *İç Denetimin gelişen ve değişen dünyasında: siber güvenlik ve denetim*, Tez (Yüksek Lisans), Marmara Üniversitesi.
- [15]. Erdinçler, R.E., 2021, *Türkiye'de ulusal güvenlik politikaları ve savunma sanayii yönetimi ilişkisi*, Tez (Yüksek Lisans), Hacettepe Üniversitesi.
- [16]. Alaca, Y., 2018, *Yapay bağımsızlık sistemleri ile bilgi güvenliği ve olay yönetimi geliştirilmesi*, Tez (Yüksek Lisans), Karabük Üniversitesi.
- [17]. Yüksel, E., 2019, *Experimenting, threat detection and SIEM integration with custom created honeypots*, Tez (Yüksek Lisans), Ankara Yıldırım Beyazıt Üniversitesi.
- [18]. İşgüzar, S., 2020, *Siber aylaklık davranışlarının bir kamu kurumu özelinde incelenmesi: log analizine dayalı bir çalışma*, Tez (Yüksek Lisans), Fırat Üniversitesi.
- [19]. Akgış, F., 2021, *Anomali tespiti için log analizi*, Tez (Yüksek Lisans), İstanbul Üniversitesi-Cerrahpaşa.
- [20]. Daş, R. ve Gündüz, M. Z., 2020, *Analysis of cyber-attacks in IoT-based critical infrastructures*, International Journal of Information Security Science, 8(4), 122-133.
- [21]. Gökçeoğlu, D., 2021, *Güvenlik bilgileri ve olay yönetimi (SIEM)/Log korelasyon kurallarının yazılması*, Tez (Doktora), Fırat Üniversitesi.
- [22]. Yerlikaya, H.N., 2020, *Log analysis of a large scale network by using Elastic Stack*, Tez (Yüksek Lisans), Bahçeşehir Üniversitesi.

- [23]. Yenal, S., ve Akdemir, N., 2020, *Uluslararası ilişkilerde yeni bir kuvvet çarpanı: siber savaşlar üzerine bir vaka analizi*, Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(1), 414-450.
- [24]. Zenginkuzucu, D.M., 2021, *Uluslararası hukuk, terörizm ve mağdur: yeni bir terörizm tanımı denemesi*, İstanbul Esenyurt Üniversitesi İşletme ve Yönetim Bilimleri Fakültesi Sosyal Bilimler Araştırmaları Dergisi, 1(2), 1-17.
- [25]. Sandılaç, N., 2021, *Siber dünyada hacker kültürü, hacktivizm ve bilişim suçları*, Tez (Yüksek Lisans), Sakarya Üniversitesi.
- [26]. Şahin, G. ve Güngörsen, R., 2021, *2001 sonrası NATO'nun terörizmle mücadele unsur, araç ve politikalarının küresel güvenliğe etkisi*, Güvenlik Bilimleri Dergisi, 10(2), 397-424.
- [27]. Demirci, K., 2021, *Kritik altyapılarda siber güvenlik ve afet üzerinden bir değerlendirme*, Nazilli İktisadi ve İdari Bilimler Fakültesi Dergisi, 2(2), 54-64.
- [28]. Shafqat, N. ve Masood, A., 2016, *Comparative analysis of various national cyber security strategies*, International Journal of Computer Science and Information Security, 14(1), 129.
- [29]. Rizal, M. Ve Yani, Y., 2016, *Cybersecurity policy and its implementation in Indonesia*, Journal of ASEAN Studies, 4(1), 61-78.
- [30]. Tomic, D., Saljic, E. ve Cupic, D., 2018, *Cyber-security policies of east european countries*, Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense, Springer, Cham.
- [31]. Sunkpho, J., Ramjan, S. ve Ottamakorn, C., 2018, *Cybersecurity policy in ASEAN countries*, In 17th Annual Security Conference, 1-7.
- [32]. Hashim, M.S., 2011, *Malaysia's national cyber security policy: The country's cyber defence initiatives*, In 2011 Second Worldwide Cybersecurity Summit (WCS), 1-7, IEEE.
- [33]. Hwang, J. ve Choi, K.S., 2021, *North Korean cyber attacks and policy responses: an interdisciplinary theoretical framework*, International Journal of Cybersecurity Intelligence & Cybercrime, 4(2), 4-24.
- [34]. Plotnek, J.J. ve Slay, J., 2021, *Cyber terrorism: a homogenized taxonomy and definition*, Computers & Security, 102, 102145.
- [35]. Broeders, D., Cristiano, F. ve Weggemans, D., 2021, *Too close for comfort: cyber terrorism and information security across national policies and international diplomacy*, Studies in Conflict & Terrorism, 1-28.
- [36]. Jangada Correia, V., 2022, *An explorative study into the importance of defining and classifying cyber terrorism in the United Kingdom*, SN Computer Science, 3(1), 1-31.
- [37]. Tamerin, A.S.A., Bakar, N.A.A., Hassan, N.H. ve Maarop, N., 2021, *Counter-narrative cyber security model to address the issues of cyber terrorism*, Open International Journal of Informatics, 9(2), 39-56.
- [38]. Shandler, R., Gross, M.L., Backhaus, S. ve Canetti, D., 2021, *Cyber terrorism and public support for retaliation—a multi-country survey experiment*, British Journal of Political Science, 1-19.
- [39]. Diorditsa, I., Katerynychuk, K., Telestakova, A., Kulak, N. ve Nastiuk, A., 2021, *Cyberterrorism as a threat to the cyber security of Ukraine: a discussion of theoretical aspects*, Amazonia Investiga, 10(40), 73-83.
- [40]. Alshabib, H.N. ve Martins, J.T., 2021, *Cybersecurity: perceived threats and policy responses in the gulf cooperation council*, IEEE Transactions on Engineering Management, 1-12.

- [41]. Abiodun, A., 2021, *A comparative analysis of the legal framework for the criminalization of cyberterrorism in Nigeria, England and the United States*, Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 12(1), 99-112.
- [42]. Darıcı, A.B., 2019, *Türkiye'nin siber güvenlik politikalarının analizi; Türkiye'nin potansiyel siber güvenlik stratejisi*, TESAM Akademi, 6(2), 11-33.
- [43]. Savaş, S. ve Karataş, S., 2022, *Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance*, International Cybersecurity Law Review, 1-28.
- [44]. Göçoğlu, V., 2018, *Türkiye'nin siber güvenlik politikalarının kamu politikası analizi çerçevesinde değerlendirilmesi*, Tez (Doktora), Hacettepe Üniversitesi.
- [45]. Alioğlu, S.D., 2019, *Siber saldırılar ve ülkelerin siber güvenlik politikaları*, Tez (Yüksek Lisans), İstanbul Bilgi Üniversitesi.
- [46]. Köksoy, F., 2020, *Avrupa Birliği'nin siber güvenlik politikası: kurumsalcılık mı tutarlılık mı?*, Güvenlik Stratejileri Dergisi, 16(35), 635-674.
- [47]. Şeker, E. ve Tolga, İ.B., 2019, *National cyber security organisation: Türkiye*, National Cyber Security Governance Series, 1-20.
- [48]. Senol, M. ve Karacuha, E., 2020, *Creating and implementing an effective and deterrent national cyber security strategy*, Journal of Engineering, 2020.
- [49]. Bilim ve İletişim Teknolojileri Dairesi, *e-Dönüşüm Türkiye projesi*, <http://www.bilgitoplumu.gov.tr/bilgi-toplumu/e-donusum-projesi/> [Erişim Tarihi: 25 Nisan 2022].
- [50]. Bilim Sanayi ve Teknoloji Bakanlığı, 2017, *Siber güvenlik kurulu* <https://www.btk.gov.tr/siber-guvenlik-kurulu>, [Erişim Tarihi: 25 Nisan 2022].
- [51]. Goztepe, K., Kilic, R. ve Kayaalp, A., 2014, *Cyber defense in depth: designing cyber security agency organization for Türkiye*, Journal of Naval Science and Engineering, 10(1), 1-24.
- [52]. Bilim Sanayi ve Teknoloji Bakanlığı, *Türkiye yazılım sektörü stratejisi ve eylem planı (2017-2019)*, 2017, Resmi Gazete, 29939.
- [53]. Alaybeyoğlu, A. ve Morkaya, Ö., 2006, *Ülkemizdeki bilgisayar mühendisliği lisans eğitimiyle yazılım mühendisliği lisans eğitiminin karşılaştırılması*, *Proceedings of the 3. Ulusal Elektrik Elektronik Bilgisayar Mühendislikleri Eğitimi Sempozyumu*, 1-4.
- [54]. Tarım, B., 2021, *Gelişmiş ülkelerin bilişim teknolojileri ve yazılım dersleri hedeflerine türkiye'de 8. ve 12. sınıf öğrencilerinin ulaşma düzeyleri*, Tez (Doktora), Hacettepe Üniversitesi.
- [55]. Yüksek Öğrenim Kurumu (YÖKATLAS), 2022, *Yazılım mühendisliği programı bulunan üniversiteler*, <https://yokatlas.yok.gov.tr/lisans-bolum.php?b=10233>, [Erişim Tarihi: 15 Nisan 2022].
- [56]. Karasoy, H.A. ve Babaoğlu, P., 2021, *Türkiye'de siber güvenlik: yasal ve kurumsal altyapı*, Yasama Dergisi, (44), 123-155.
- [57]. Bıçakçı, S., Ergun, D. ve Çelikkpala, M., 2015, *Türkiye'de siber güvenlik*, Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi, 1, 1-35.
- [58]. *Elektronik İmza Kanunu*, Resmi Gazete 8719 (15 Ocak 2004), Kanun No. 5070, md.3, <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5070.pdf>, [Erişim Tarihi: 07 Mayıs 2022].
- [59]. *Türk Ceza Kanunu*, Resmi Gazete 8965 (26 Eylül 2004), Kanun No. 5237, md. 1-3, <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf> [Erişim Tarihi: 07 Mayıs 2022].
- [60]. *Terörle Mücadele Kanununda Değişiklik Yapılmasına Dair Kanun*, Resmi Gazete (29 Haziran 2006), Kanun No. 5532, <https://www.resmigazete.gov.tr/eskiler/2006/07/20060718-1.htm>, [Erişim Tarihi: 07 Mayıs 2022].

- [61]. *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*, Resmi Gazete 26530 (04 Mayıs 2007), Kanun No. 5651, md. 1-2, <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf>, [Erişim Tarihi: 06 Mayıs 2022].
- [62]. *Elektronik haberleşme Kanunu*, resmi gazete 27050 (05 Kasım 2008), Kanun no. 5809, md. 1-3, <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf>, [Erişim Tarihi: 07 Mayıs 2022].
- [63]. *Kişisel verilerin korunması kanunu*, Resmi gazete 29677 (24 Mart 2016), Kanun no. 6698, md. 1-4, <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf>, [Erişim Tarihi: 07 Mayıs 2022].
- [64]. Moualla, S., Khorzom, K., ve Jafar, A., 2021, *Improving the performance of machine learning-based network intrusion detection systems on the UNSW-NB15 dataset*, Computational Intelligence and Neuroscience, 2021.
- [65]. Zoghi, Z., ve Serpen, G., 2021, *UNSW-NB15 computer security dataset: Analysis through visualization*, arXiv preprint arXiv:2101.05067.
- [66]. Aleesa, A. M., Mohammed, Y., Mohammed, A.A., ve Sahar, N., 2021, *Deep-intrusion detection system with enhanced UNSW-NB15 dataset based on deep learning techniques*, Journal of Engineering Science and Technology, 16(1), 711-727.
- [67]. Kocher, G., ve Kumar, G., 2021, *Analysis of machine learning algorithms with feature selection for intrusion detection using UNSW-NB15 dataset*, International Journal of Network Security & Its Applications (IJNSA), 13(1).
- [68]. Mahalakshmi, G., Uma, E., Aroosiya, M., ve Vinitha, M., 2021, *Intrusion detection system using convolutional neural network on UNSW NB15 dataset*, In Advances in Parallel Computing Technologies and Applications, 1-8.
- [69]. Abdullah, Iqbal, F.B., Biswas, S., ve Urba, R., 2021, *Performance analysis of intrusion detection systems using the PyCaret machine learning library on the UNSW-NB15 dataset*, Tez (Doktora), Brac Üniversitesi.
- [70]. Sharma, N., Yadav, N. S., ve Sharma, S., 2021, *Classification of UNSW-NB15 dataset using exploratory data analysis using ensemble learning*, EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 8(29).
- [71]. Sarhan, M., Layeghy, S., ve Portmann, M., 2022, *Towards a standard feature set for network intrusion detection system datasets*, Mobile Networks and Applications, 27(1), 357-370.
- [72]. Pacheco, Y., ve Sun, W., 2021, *Adversarial machine learning: a comparative study on contemporary intrusion detection datasets*, In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, 160-171.
- [73]. Kilincer, I.F., Ertam, F. Ve Sengur, A., 2021, *Machine learning methods for cyber security intrusion detection: datasets and comparative study*, Computer Networks, 188, 107840.
- [74]. Kushwah, G.S., ve Ranga, V., 2021, *Optimized extreme learning machine for detecting DDoS attacks in cloud computing*, Computers & Security, 105, 102260.
- [75]. Roy, S., Mandal, A., Dey, D., 2021, *Intelligent intrusion detection system using supervised learning*. *AIJR Proceedings*, 25-34.
- [76]. Ahsan, M., Gomes, R., Chowdhury, M., ve Nygard, K.E., 2021, *Enhancing machine learning prediction in cybersecurity using dynamic feature selector*, Journal of Cybersecurity and Privacy, 1(1), 199-218.
- [77]. Pooja, T.S., ve Shrinivasacharya, P., 2021, *Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security*, *Global Transitions Proceedings*, 2(2), 448-454.

- [78]. Thirimanne, S., Jayawardana, L., Liyanaarachchi, P., ve Yasakethu, L., 2021, Comparative algorithm analysis for machine learning based intrusion detection system, *10th International Conference on Information and Automation for Sustainability (ICIAfS)*, 191-196, IEEE.
- [79]. Rani, M., 2022, *Effective network intrusion detection by addressing class imbalance with deep neural networks multimedia tools and applications*, *Multimedia Tools and Applications*, 81(6), 8499-8518.
- [80]. Ozkan-Okay, M., Aslan, Ö., Eryigit, R., ve Samet, R., 2021, *SABADT: hybrid intrusion detection approach for cyber attacks identification in WLAN*, *IEEE Access*, 9, 157639-157653.
- [81]. Sekhar, R., Sasirekha, K., Raja, P. S. ve Thangavel, K., 2021, *A novel GPU based intrusion detection system using deep autoencoder with Fruitfly optimization*, *SN Applied Sciences*, 3(6), 1-16.
- [82]. Yang, S.U., 2021, Research on network malicious behavior analysis based on deep learning, *IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 5, 2609-2612, IEEE.
- [83]. Han, H., Kim, H. ve Kim, Y., 2022, *An efficient hyperparameter control method for a network intrusion detection system based on proximal policy optimization*, *Symmetry*, 14(1), 161.
- [84]. Al-Gethami, K.M., Al-Akhras, M.T.ve Alawairdhi, M., 2021, *Empirical evaluation of noise influence on supervised machine learning algorithms using intrusion detection datasets*, *Security and Communication Networks*, 2021.
- [85]. Meliboev, A., Alikhanov, J. ve Kim, W., 2022, *Performance evaluation of deep learning based network intrusion detection system across multiple balanced and imbalanced datasets*, *Electronics*, 11(4), 515.
- [86]. El-Sayed, O.A., Fawzy, S.K., Tolba, S.H., Salem, R.S., Hassan, Y.S., Ahmed, A.M. ve Khattab, A., 2021, Deep learning framework for accurate network intrusion detection in ITSs, *2021 International Conference on Microelectronics (ICM)*, 212-215, IEEE.
- [87]. Kim, S., Chen, L. ve Kim, J., 2021, Intrusion Prediction using Long Short-Term Memory Deep Learning with UNSW-NB15, *2021 IEEE/ACIS 6th International Conference on Big Data, Cloud Computing and Data Science (BCD)*, 53-59, IEEE.
- [88]. Hossain, Z., Sourov, M.M.R., Khan, M. ve Rahman, P., 2021, Network Intrusion Detection using Machine Learning Approaches, *Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 438-442, IEEE.
- [89]. Dutt, I., 2021, *Pre-Processing of KDD'99 & UNSW-NB network intrusion datasets*, *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(11), 1762-1776.
- [90]. Kim, S., Chen, L. ve Kim, J., 2021, Intrusion Prediction using LSTM and GRU with UNSW-NB15, *In 2021 Computing, Communications and IoT Applications (ComComAp)*, 101-106, IEEE.
- [91]. Singh, R. ve Srivastav, G., 2021, Novel Framework for Anomaly Detection Using Machine Learning Technique on CIC-IDS2017 Dataset, *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, 632-636, IEEE.
- [92]. Silva, J.V.V., de Oliveira, N.R., Medeiros, D.S., Lopez, M.A. ve Mattos, D.M., 2022, *A statistical analysis of intrinsic bias of network security datasets for training machine learning mechanisms*, *Annals of Telecommunications*, 1-17.
- [93]. Priya, S., 2021, *Performance analysis comparison on various cyber-attack dataset by relating a deep belief network model on an intrusion detection system (IDS)*, *Information Technology in Industry*, 9(3), 608-613.

- [94]. Man, J. ve Sun, G., 2021, *A residual learning-based network intrusion detection system*, Security and Communication Networks, 2021.
- [95]. Ashiku, L. ve Dagli, C., 2021, Network intrusion detection system using deep learning, *Procedia Complex Adaptive Systems Conference*, 185, 239-247.
- [96]. Hooshmand, M. K. ve Hosahalli, D., 2022, *Network anomaly detection using deep learning techniques*, CAAI Transactions on Intelligence Technology, 1-16.
- [97]. Kamarudin, I.E., Ab Razak, M.F., Firdaus, A., Jaya, M. I. ve Dun, Y.T., 2021, Performance Analysis on Denial of Service attack using UNSW-NB15 Dataset, 2021 *International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, 423-426, IEEE.
- [98]. Magán-Carrión, R., Urda, D., Díaz-Cano, I., ve Dorronsoro, B., 2021, *Improving the Reliability of Network Intrusion Detection Systems through Dataset Integration*, IEEE Transactions on Emerging Topics in Computing, 1-15.
- [99]. Sharma, N. ve Yadav, N.S., 2021, Ensemble Learning based Classification of UNSW-NB15 dataset using exploratory data analysis, *9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, 1-7, IEEE.
- [100]. Chew, Y.J., Lee, N., Ooi, S.Y., Wong, K.S. ve Pang, Y.H., 2021, *Benchmarking full version of GureKDDCup, UNSW-NB15, and CIDDs-001 NIDS datasets using rolling-origin resampling*, Information Security Journal: A Global Perspective, 1-22.
- [101]. Acharya, T., Khatri, I., Annamalai, A., ve Chouikha, M.F., 2021, Efficacy of Machine Learning-Based Classifiers for Binary and Multi-Class Network Intrusion Detection, *2021 IEEE International Conference on Automatic Control & Intelligent Systems (I2CACIS)*, 402-407, IEEE.
- [102]. Dlamini, G. ve Fahim, M., 2021, *DGM: a data generative model to improve minority class presence in anomaly detection domain*, Neural Computing and Applications, 33(20), 13635-13646.
- [103]. Pavlov, A. ve Voloshina, N., 2021, Dataset selection for attacker group identification methods, *30th Conference of Open Innovations Association FRUCT*, 171-176, IEEE.
- [104]. Güler, H. ve Alpay, Ö., 2021, Intrusion Detection and Classification Based on Deep Learning, *2021 International Conference on Information Security and Cryptology (ISCTURKIYE)*, 40-44, IEEE.
- [105]. Gürtürk, U., Baykara, M., ve Karabatak, M., 2017, *Identifying the visitors with data mining methods from web log files*, International Journal of Emerging Technologies in Engineering Research (IJETER), 5(3), 243-249.
- [106]. Kuroki, M., 2021, *Using Python and Google Colab to teach undergraduate microeconomic theory*, International Review of Economics Education, 38, 100225.
- [107]. Canesche, M., Bragança, L., Neto, O. P. V., Nacif, J. A. ve Ferreira, R., 2021, Google colab cad4u: hands-on cloud laboratories for digital design, *In 2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, 1-5.
- [108]. Alnajjar, M., 2021, *Image-based detection using deep learning and google colab*, International Journal of Academic Information Systems Research (IJASIR), 5(1), 30-35.
- [109]. Google colabratory-Google, 2017, *Open in clolab*, <https://chrome.google.com/webstore/detail/open-in-colab/iogfkhleblhpcckbiedikdehleodpjo>, [Erişim Tarihi: 18 Mayıs 2022].

- [110]. Joseph, T. ve Scholar, P.G., 2021, Placement prediction of students using the data mining tool weka, *In Proceedings of the National Conference on Emerging Computer Applications (NCECA)*, 3(1), 251-253.
- [111]. Kisi, O., Shiri, J., Karimi, S., Shamshirband, S., Motamedi, S., Petković, D.ve Hashim, R., 2015, *A survey of water level fluctuation predicting in Urmia Lake using support vector machine with firefly algorithm*, *Applied Mathematics and Computation*, 270, 731-743.
- [112]. Acharya, T. D., 2018, *Regional scale landslide hazard assessment using machine learning methods in Nepal*, Tez (Doktora), Kangwon National University.
- [113]. Chakrabarty, N. ve Biswas, S., 2020, *Navo minority over-sampling technique (NMOTe): a consistent performance booster on imbalanced datasets*, *Journal of Electronics*, 2(02), 96-136.
- [114]. Ertam, F., 2017, *Sosyal medya verileri için etkili bir sınıflandırma yaklaşımı*, *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 29(2), 67-73.
- [115]. Raschka, S., 2022, *Machine learning FAQ*, <https://sebastianraschka.com/faq/docs/logisticregr-neuralnet.html#what-is-the-relation-between-logistic-regression-and-neural-netw>, [Erişim Tarihi: 18 Mayıs 2022].
- [116]. Baykara, M., Daş, R. ve Tuna, G., 2016, *Web sunucu erişim kütüklerinden web ataklarının tespiti için yönelik web tabanlı log analiz platformu*, *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 28(2), 291-302.