İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

AĞ DAVRANIŞ MODELİ İLE KURUM İÇİ SALDIRILARIN BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Ayşe GÜL

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

ARALIK 2018

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

AĞ DAVRANIŞ MODELİ İLE KURUM İÇİ SALDIRILARIN BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Ayşe GÜL
(707151030)

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Prof. Dr. Ertuğrul KARAÇUHA
Eş Danışman: Prof. Dr. Eşref ADALI

ARALIK 2018

İTÜ, Bilişim Enstitüsü'nün 707151030 numaralı Yüksek Lisans Öğrencisi Ayşe GÜL, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "AĞ DAVRANIŞ MODELİ İLE KURUM İÇİ SALDIRILARIN BELİRLENMESİ" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Ertuğrul KARAÇUHA** İstanbul Teknik Üniversitesi	.....
Eş Danışman :	**Prof. Dr. Eşref ADALI** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. İbrahim SOĞUKPINAR** Gebze Teknik Üniversitesi	.....
	Doç. Dr. M. Oğuzhan KÜLEKCİ İstanbul Teknik Üniversitesi	.....
	Dr. Öğr. Üyesi Şerif BAHTİYAR İstanbul Teknik Üniversitesi	.....

Teslim Tarihi : 15 Kasım 2018
Savunma Tarihi : 14 Aralık 2018

Aileme ve arkadaşlarıma,

ÖNSÖZ

Tez çalışmam sırasında gösterdiği her türlü ilgi, destek ve anlayış için değerli danışman hocam sayın Prof. Dr. Ertuğrul KARAÇUHA'ya, kıymetli bilgi, birikim ve tecrübeleri ile beni yönlendiren ve insani ve ahlaki değerleri ile örnek edindiğim değerli eş danışman hocam sayın Prof. Dr. Eşref ADALI 'ya, bu günlere gelmemde büyük pay sahibi olan ve beni hiçbir zaman yalnız bırakmayan aileme ve destek ve yardımlarını esirgemeyen dostlarıma sonsuz teşekkürler ederim.

Kasım 2018

Ayşe GÜL
Bilgisayar Mühendisi

İÇİNDEKİLER

Sayfa

ÖNSÖZ ..... **vii**
İÇİNDEKİLER ..... **ix**
KISALTMALAR ..... **xi**
ÇİZELGE LİSTESİ ..... **xiii**
ŞEKİL LİSTESİ ..... **xv**
ÖZET ..... **xvii**
SUMMARY ..... **xix**
1. GİRİŞ **1**
1.1 Tezin Amacı 4
1.2 Kaynak Araştırması 5
1.2.1 Güvenlik Gereksinimlerinin Çözümlenmesi 5
1.2.2 Saldırıların Belirlenmesi 9
1.3 Tezin Katkısı 14
1.4 Tezin Düzeni 14
2. SALDIRILAR VE GÜVENLİK AÇIKLIKLARI **17**
2.1 Siber Güvenlik Saldırı Türleri 19
2.1.1 Varlıklara yönelik saldırılar 19
2.1.2 Sisteme yönelik saldırılar 21
2.1.3 Kişilere yönelik saldırılar 23
2.1.3.1 Çalışana yönelik saldırılar 23
2.1.3.2 Müşteriye yönelik saldırılar 24
2.1.4 Kuruma yönelik saldırılar 24
2.2 Güvenlik Açıklıkları 24
2.2.1 Bilinçli açıklıklar 24
2.2.2 Bilinçsiz açıklıklar 24
2.2.2.1 Sistem açıklıkları 24
2.2.2.2 Çalışan hatası 25
3. SALDIRI BELİRLEME YÖNTEMLERİ **27**
3.1 A-NIDS Teknikleri 28
3.1.1 İstatiksel temelli yaklaşım 29
3.1.2 Bilgi temelli yaklaşım 30
3.1.3 Makine öğrenmesi yaklaşımı 31
3.2 Derin Öğrenme 32
3.3 Ağ Davranış Çözümlemesi 34
4. GELİŞTİRİLEN YÖNTEM **35**
4.1 Veri Kümesi 36
4.2 Verilerin İncelenmesi ve Özniteliklerin Çıkarılması 38
4.3 Model Oluşturma 43
4.4 Değerlendirme 46
4.4.1 Çizelge A.2 ’de yer alan özniteliklerin kullanımıyla elde edilen sonuçlar 46

4.4.2 Çizelge A.2 ’de yer alan özniteliklerin kullanımıyla elde edilen sonuçlar 50
5. SONUÇ VE ÖNERİLER 53
5.1 Yürütülen Çalışma 53
5.2 İleriki Çalışmalar 53
KAYNAKLAR 55
EKLER 59
ÖZGEÇMİŞ 73

KISALTMALAR

A-NIDS	**:** Anomaly-Based Network Intrusion Detection System
ANN	**:** Artificial Neural Network
CAPEC	**:** Common Attack Pattern Enumeration and Classification
CIDF	**:** Common Intrusion Detection Framework
CVE	**:** Common Vulnerabilities and Exposures
DARPA	**:** Defense Advanced Research Projects Agency
IAP	**:** Intrusion Alert Protocol
IDS	**:** Intrusion Detection System
IDGW	**:** Intrusion Detection Working Group
IDMEF	**:** Intrusion Detection Message Exchange Format
IDXP	**:** Intrusion Detection EXchange Protocol
IETF	**:** Internet Engineering Task Force
ISCX	**:** Information Security Center of Excellence
LDAP	**:** Lightweight Directory Access Protocol
NAT	**:** Network Address Resolution
NBAD	**:** Network Behaviour Anomaly Detection
NIDS	**:** Network Intrusion Detection System
RADIUS	**:** Remote Authentication Dial-In User Service
SIEM	**:** Security Information and Event Management
SMB	**:** Server Message Block
STS	**:** Sosyo-Teknik Sistemler

ÇİZELGE LİSTESİ

Sayfa

Çizelge 1.1 : STRIDE tehdit modeli. 7
Çizelge 3.1 : Makine öğrenmesi algoritmaları. 32
Çizelge 4.1 : Veri kümesi günlük veri boyutları. 37
Çizelge 4.2 : Veri kümesinde yer alan protokoller. 39
Çizelge 4.3 : Akış verileri. 41
Çizelge 4.4 : Model oluşturma sürecinde üretilen maliyet değerleri. 47
Çizelge 4.5 : Model oluşturma sürecinde üretilen maliyet değerleri. 48
Çizelge A.1 : Pcap dosyasından çıkarılan veri türleri. 61
Çizelge A.2 : Öğrenme algoritmasında kullanılan öznitelikler. 63
Çizelge A.3 : Önemi yüksek öznitelikler. 65
Çizelge A.4 : Sözlük. 67

ŞEKİL LİSTESİ

Sayfa

Şekil 1.1 : Güvenlik özniteliği hiyerarşisi. 6
Şekil 1.2 : Yetki yükseltme saldırısı için uygulanabilir saldırı modeli. 8
Şekil 1.3 : CIDF tarafından oluşturulan ortak çerçeve. 10
Şekil 2.1 : İç tehdit türleri. 18
Şekil 2.2 : Kurum içi saldırı türleri. 19
Şekil 2.3 : İç saldırılar için savunmasız veri türleri. 20
Şekil 2.4 : Bilgi sistemlerinin korunmasızlık oranı. 22
Şekil 3.1 : Genel fonksiyonel mimari. 28
Şekil 3.2 : Yapay sinir ağları. 33
Şekil 4.1 : Makine öğrenmesi süreçleri. 35
Şekil 4.2 : Sınama ortamı ağ mimarisi. 37
Şekil 4.3 : Editcap.exe ekran görüntüsü. 38
Şekil 4.4 : Wireshark ağ izleme aracı. 39
Şekil 4.5 : Kullanılacak verilerin TShark ile .csv formatına dönüştürülmesi. 40
Şekil 4.6 : Bağdaşma grafik haritası. 42
Şekil 4.7 : Önemi yüksek özniteliklerin oran grafiği. 43
Şekil 4.8 : ANN grafik gösterimi. 45
Şekil 4.9 : Eğitim ve sınama verilerinin maliyet grafiği. 47
Şekil 4.10 : Eğitim ve sınama verilerinin maliyet grafiği. 48
Şekil 4.11 : 47 öznitelik içeren sınama verilerinin birleştirilmiş maliyet grafiği. 49
Şekil 4.12 : 47 özniteliğe ilişkin sınama verileri azaltılmış maliyet grafiği. 49
Şekil 4.13 : 19 öznitelik içeren sınama verilerinin birleştirilmiş maliyet grafiği. 50
Şekil 4.14 : 19 ve 47 özniteliklerine sahip sınama verilerinin maliyet grafiği. 51
Şekil A.1 : 47 öznitelik ve farklı gizli nöron sayıları ile üretilen maliyet grafikleri: (a)20-100-50. (b)50-100-50. (c)100-400-20. (d)100-400-200. (e)150-300-150. (f)200-300-200. 69
Şekil A.2 : 19 öznitelik ve farklı gizli nöron sayıları ile üretilen maliyet grafikleri: (a)20-100-50. (b)50-100-50. (c)100-400-20. (d)100-400-200. (e)150-300-150. (f)200-300-200. 71

AĞ DAVRANIŞ MODELİ İLE KURUM İÇİ SALDIRILARIN BELİRLENMESİ

ÖZET

Günümüzde yetkili kişiler tarafından yapılan saldırıların ya da yetkili kişilerin özensizliği sonucunda oluşan güvenlik açıklıklarının, dışarıdan yapılan saldırılara göre daha çok zarara neden olduğu görülmektedir. Kurumlar kendileri için değerli olan varlıkları korumak adına veri sızıntısı önleme, şifreleme, kimlik ve erişim kontrolü gibi yaygın güvenlik çözümlerini kullanmaktadır. Ancak gelişmiş sürekli tehditlerin (APT), geleneksel güvenlik çözümlerini atlatan saldırıların ve iç sistemler ile uyumlu çalışan bilinmeyen kötü amaçlı yazılımların artması güvenlik çözümlerinin ve ortamlarının değişmesine neden olmaktadır. Bu kapsamda içeriden gelen tehditlerin ve saldırıların daha iyi belirlenebilmesi için eylem tutanağı (log) yönetimi ve saldırı belirleme ve önleme sistemleri (IDS / IPS) kullanılmaktadır.

Bu çalışma saldırı belirleme sistemlerine yoğunlaşarak iç tehditlerin ve saldırıların belirlenmesine yönelik yapılan araştırma ve geliştirmeyi içermektedir.

Geleneksel saldırı belirleme sistemleri, imza temelli ya da olağan dışı durum temelli yaklaşımlar kullanılarak tasarlanmaktadır. İmza temelli sistemler, incelenen veriler içerisinde tanımlanmış kalıpları ya da imzaları bulmaya çalışmaktadır. Bu amaçla bilinen saldırılara karşılık gelen kalıplar için bir veri tabanı oluşturulmaktadır. Bu sistemlerde, belirlenmiş ve bilinen saldırıların belirlenme oranı çok yüksek olmasına karşın yeni ve bilinmeyen saldırıların belirlenmesinde yetersiz kalmaktadır.

Olağan dışı durum temelli sistemler, korunacak sistemin olağan davranışını öngörmeye çalışmakta ve belirli bir anda gözlemlediği davranış ile olağan davranış arasındaki sapmaya bakmaktadır. Bu yaklaşımda gözlemlenen sapma önceden tanımlanmış bir eşiği aştığında olağan dışı durum uyarısı üretilmektedir. Bu sistemlerin en önemli üstünlüğü daha önce görülmemiş saldırı olaylarını belirlemedeki başarısıdır.

İmza temelli ve olağan dışı durum temelli saldırı belirleme yöntemlerinde ağ üzerindeki her paket incelenerek bir sonuç üretilmektedir. Paketin kaçırıldığı ya da doğru sonucun üretilmediği durumlarda ise ağ üzerindeki tehdit devam etmektedir. Bu problemin çözümü için ise ağ davranış çözümlemesi yaklaşımı kullanılmaktadır.

Ağ davranış çözümlemesi yaklaşımında pasif olarak ağda meydana gelen durumlar izlenmekte ve saldırı olarak değerlendirilebilecek bilinmeyen, yeni oluşan ya da olağan dışı durumlar işaretlenmektedir. Bu yaklaşımın diğer saldırı belirleme yöntemlerinden farkı ağda gördüğü her paket için değil, paketlerin bir araya getirilmesiyle oluşturulan veri akışına bakarak bir sonuç üretmesidir. Ayrıca bu yaklaşım daha çok iç ağlara odaklanmaktadır.

Bu çalışmada içeriden oluşan tehditlerin belirlenmesi amacıyla veri akış bilgisi kullanılarak olağan dışı durumları işaretleyen Ağ Davranışlarında Olağan Dışı

Durumların Belirlenmesi (Network Behaviour Anomaly Detection - NBAD) yaklaşımına odaklanılmıştır.

Çalışmanın yürütülmesi için ağ trafik bilgisini içeren bir veri kümesine ihtiyaç duyulmaktadır. Bu kapsamda Wireshark ağ izleme aracı ile yedi gün boyunca ağ trafiği izlenerek oluşturulmuş UNB ISCX IDS 2012 veri kümesi kullanılmıştır. Bu veri kümesinde yer alan ağ paketleri kullanılarak veri akışı oluşturulmuştur.

Oluşturulan veri akışı üzerinde olağan dışı durumların belirlenmesi için makine öğrenmesinin bir alt kümesi olan derin öğrenme algoritmaları kullanılmıştır.

Derin öğrenme, insan beyninin yapısı ve işlevselliği esinlenerek oluşturulmuş yapay sinir ağlarını içermektedir. Yapay sinir ağlarının eğitilmesi için çok sayıda veriye ve yüksek işlem kapasitesine sahip bilgisayarlara ihtiyaç duyulmaktadır. Bu nedenle yapay sinir ağları eskiden geliştirilmiş bir algoritma olmasına karşın kullanımı özellikle TensorFlow kütüphanesinin geliştirilmesiyle birlikte son dönemde artmıştır.

Çalışma kapsamında veri kümesinde yer alan bilgiler değerlendirilerek 47 adet öznitelik belirlenmiş ve bu öznitelikleri içeren veri akışı oluşturulmuştur. Hazırlanmış veri akışı ve yapay sinir ağları algoritması kullanılarak en iyi sonucu üreten modelin oluşturulması amaçlanmıştır. Bu kapsamda algoritmaya ait katman ve nöron sayıları değiştirilerek üretilen sonuçlar karşılaştırılmış ve en iyi sonucun 3 gizli katmanlı ve 100-400-200 düğüm değerleri ile %98.44 oranında doğruluk sonucunun üretildiği görülmüştür.

DETECTION OF INSIDER ATTACKS USING NETWORK BEHAVOUR MODEL

SUMMARY

An attack is an information security threat that involves an attempt to gain unauthorized access to information resource or services, or to obtain, reveal, remove, alter or destroy sensitive information.

There are two types of attacks as passive and active attacks. Passive attacks are used to get information without hurting system resources. Therefore, the detection of these attacks are pretty difficult. Generally, in this attack type network communication is eavesdropped to make a traffic analysis and release of message content. On the other hand, active attacks are used to change or remove information, alter or destroy system resources and prevent system operations. The most known active attacks are masquerade, modification of messages, repudiation, session replay, and denial of service.

Information security is a growing concern and protection of the sensetive data has been becoming more difficult issue because of the ever-growing complex structures of information systems. A security vulnerability in any component of the system can cause serious security problems. Moreover, attackers who know these vulnerabilities can damage the system. Most institutions or organizations have been continuously damaged by attacks. Therefore, Information Technology (IT) security teams of institutions have focused on detecting attacks and stopping intruders from gaining access to assets on the corporate network.

Attacks are categorized as an internal and external attack based on the identity of the attacker.

External attacks are performed to find network vulnerabilities, gain access on information system and capture sensitive data by someone who is skilled and sophisticated from outside of the institution.

On the other hand, internal attacks are performed by someone who is close to an organization with authorized access and misuses that access negatively to impact the organization’s critical information or system. An insider can be a current or former employee, contractor, or business partner who has or had authorized access to the organization’s network, systems, or data.

Threat and attack are the two terms associated with internal attacks. Insider threat can be occur because of negligance of employee, so it is not referred as attack directly. It is called attack when someone tries to harm the system intentionally. In contrast, it is called insider threat when some error occurs unintentionally because of employee mistakes which creates a vulnerability on the system and puts a risk on it. Besides, operating system vulnerabilities which are currently published on Common Vulnerabilities and Exposures (CVE) are referred as threat for a system.

Nowadays, it is seen that the attacks by authorized people or security vulnerabilities because of negligence or lack of knowledge of authorized people caused more damage than the external attacks. Institutions or organizations use common security solutions such as Data Loss Prevention (DLP), encryption, and identity and access management solutions to protect assets which are valuable to them. However, security solutions and environments have started to change as a result of the rise of advanced persistent threats (APT), increased attacks that bypass traditional security solutions and unknown malwares which can run without affecting the internal systems. For this reason, Intrusion Detection and Prevention Systems (IDS / IPS), log management and SIEM platforms have been developed and used by institutions to provide a better detection of insider threats and attacks.

This study comprises of research and development to detect internal threats and attacks by focusing on intrusion detection systems.

Traditional intrusion detection systems have been designed and developed using signature-based detection and anomaly-based detection approaches. Signature-based detection systems try to find defined patterns or signatures within the examined data. For this purpose, a database have been effectuated for patterns or signatures corresponding to known attacks. In these systems, although the rate of detection of the identified and known attacks is very high, it is insufficient to identify new and unknown attacks.

Anomaly-based systems predicts the unusual behavior of the protected system and determines the deviation between the behavior that is observed at a given moment and the usual behavior. This approach also generates an unusual status warning when the observed deviation exceeds a predefined threshold. The most important advantage of these systems is the success in detecting unseen attacks.

Signature-based detection and anomaly-based detection methods both examines each network packet and produces a result. In the situation that the packet has been missed or the correct result has not been produced, the threat on the network continues. Network Behaviour Analysis (NBA) approach is used in order to solve this problem.

Network behavior analysis approach passively monitors the traffic on network and marks the new, unknown, or unusual situations which can be considered as an attack. The difference between this approach and the other detection methods is that it produces a result by examining the data flow generated by combining the network packets. Also this approach generally focuses on internal networks.

In this study, we focused on the Network Behavior Anomaly Detection (NBAD) approach which detects new and unusual situations by using data flow information in order to detect internal threats.

In order to advance the study, a data set that contains network traffic information is needed. In this context, the UNB ISCX IDS 2012 data set which was created by monitoring network traffic for seven days with Wireshark network monitoring tool have been used. Also, data flow that includes source IP, destination IP, source port number and destination port number as a key was created using network packets in this data set.

After this process, deep learning approach which had been developed as a subset of machine learning have been used to detect the abnormalities.

Deep learning includes artificial neural networks inspired by the structure and functionality of the human brain. For the training of artificial neural networks, a large number of data and computers with high processing capacity are needed. Therefore, although artificial neural networks are a formerly developed algorithm, its use has increased recently, especially with the development of the TensorFlow library.

Within the scope of the study, 47 features were identified using the data set and a data flow containing these attributes was created. By using this prepared data flow and artificial neural network algorithm, it is aimed to determine the model that produces the best result by changing the layer and neuron numbers of the algorithm. Consequently, the results obtained by changing the number of layers and neurons of the algorithm were compared and it was seen that the best result was produced with 3 hidden layer and 100-400-200 neuron/node values and 98.44% accuracy result.

1. GİRİŞ

Tek başına çalışan bilgisayarlar döneminden, birbirine bağlı bilgisayarlar dönemine geçilmesiyle birlikte güvenlik sorunları görülmeye başlanmıştır. Özellikle Genelağ'ın yaygınlaşmasının sonucu olarak bilgisayar ve bilgi güvenliği önemli bir sorun olarak karşımıza çıkmaktadır. Genelağ ya da yerel ağa bağlı olan her bilgisayar artık saldırılar ile karşı karşıyadır. Bu durum, bilgisayar güvenliği konusunda yoğun çalışmaların yapılmasını gerektirmektedir. Bilgi sistemlerine yönelik saldırılar amaçları açısından şöyle sınıflandırılmaktadır [1]:

- Bilgileri öğrenme ve çalma
- Bilgileri değiştirme
- Bilgileri silme

Saldırılar etki açısından değerlendirildiğinde hedefleri şöyle açıklanmaktadır:

- Ekonomik
- Sosyal
- Politik

Bilgi sistemlerine yönelik saldırılar işleniş yeri açısından değerlendirildiğinde;

- Dışarıdan yapılan saldırılar
- İçeriden yapılan saldırılar

olarak iki kümeye ayrılmaktadır.

Dışarıdan ve içeriden yapılan saldırı türleri amaç ve etki açısından benzer olmalarına karşın işleniş biçimleri farklıdır. Bu nedenle saldırılara karşı alınacak önlemler de farklı olmaktadır. Dışarıdan yapılan saldırılar, içeriden yapılan saldırılara oranla yayın organlarında daha çok yer almaktadır. Ancak, istatistiksel veriler içeriden yapılan saldırıların daha etkili olduğunu göstermektedir. P. Marais ve P. Ostwalt tarafından yapılan araştırmanın sonucuna göre saldırıların %35'i içeriden, %18'i dışarıdan ve %43'ü her iki biçimin de kullanılması ile gerçekleştiğini göstermektedir [2]. Bu çalışmada, saldırganlardan %65'inin kurumda çalışmakta olduğu, %21'nin eski çalışan olduğu saptanmıştır. Saldırganlar görev ve yetkileri açısından değerlendirildiğinde %32'sinin yönetici, %26'sının yönetici müdür, %20'sinin çalışan, %5'nin memur, %3'ünün yönetici olmayan müdür, %3'ünün çeşitli kişiler ve %2'sinin kuruluş sahibi veya ortağı olduğu belirlenmiştir. Bu değerlendirmelere bakıldığında kurum ya da kuruluş içinden yapılan saldırıların önemi anlaşılmaktadır.

Dışarıdan yapılan saldırılar çoğunlukla solucan, Truva atı gibi virüsler kullanılarak yapılmaktadır. Amaç kurum ya da bireylere ilişkin önemli bilgileri ele geçirmek ve daha sonra bunları çıkar amaçlı kullanmaktır. Dışarıdan yapılan saldırıların bazıları bilgi sistemini çökertmeye yöneliktir. Bu amaçla robot bilgisayarlar oluşturulmaktadır. Böylece kurumlar hatta hükümetler çalışamaz duruma getirilebilmektedir. Dışarıdan yapılan saldırıların türleri ve gerçekleşiş biçimleri genellikle bilinmektedir. Önlenmeleri için güvenlik duvarı, içerik süzme (proxy), eylem tutanağı (log) gibi birçok güvenlik unsuru kullanılarak saldırılar engellenmeye çalışılmaktadır. Dış saldırılar, büyük ve küçük kuruluşlar için sürekli bir tehlike oluşturmasına karşın, bir kurumun kendi çalışanlarının, tedarikçilerinin ya da ortaklarının eylemleri daha fazla tehlikeye yol açabilmektedir.

Bu tez çalışması kuruluş ya da kurum içinden yapılan saldırıların belirlenmesi ve önlenmesi ile ilgilidir. Kuruluş ya da kurum içinden yapılan saldırılar ile ilgili bazı açıklamalar, örnekler ve etkileri aşağıda açıklanmıştır:

Bilgi çalma: Kuruluş ya da kurumun korunması gereken veriler çalınarak kurumun bilgi birikimi çalınmaktadır. Bu bilgiler rakip kuruluşlar tarafından kullanılmaktadır. Örneğin kuruluşta geliştirilen yeni bir teknoloji rakip kuruluşun eline geçebilmektedir. Bir ülkenin savunması ile ilgili gizli bilgiler düşmanın eline geçebilmektedir. Bireylere ilişkin bilgiler çalınarak, bireylere maddi ve manevi zararlar verilebilmektedir. Örneğin müşterinin banka hesaplarından para çalınabilmektedir.

Bilgi silme: Bir kuruluşun veri tabanında bulunan bir ya da daha fazla bilginin silinmesi önemli zararlara neden olabilmektedir. Örneğin bankanın bilgisayarında bir müşterinin parasal varlığının silinmesi ya da vergi dairesinin bilgisayarında bir kuruluşun vergi borcunun silinmesi önemli ekonomik sonuçlar doğurabilmektedir.

Bilgi değiştirme: Bir kuruluşun veri tabanındaki bilgilerin silinmesinden daha tehlikeli olan saldırı, verilerin değiştirilmesidir. Verilerde yapılacak değişiklik, silinmesinden daha zor ortaya çıkarılacağı için etkisi daha büyük olabilmektedir. Veri tabanındaki verileri değiştirerek gerçekleştirilen önemli soygunlardan biri "salam dilimi" olarak bilinmektedir.

Engelleme: Bilgi sisteminin çalışmasını engellemeye veya yavaşlatmaya yönelik saldırılardır. Böylece bilgi sisteminin verdiği hizmetler yavaşlatılmış veya aksatılmış olur.

Zarar verme: Bilgi sisteminde bulunan donanım veya yazılıma zarar vermek sıkça karşılaşılan saldırı türüdür. Bilgisayara yerleştirilen mantıksal bombalar zamanı gelince bir ya da tüm yazılımları veya verileri silebilmektedir.

İnsanların bilgi sistemlerine neden saldırdıkları araştırıldığında, en önemli dürtünün %66 ile maddi kazanç elde etmek olduğu görülmüştür. İkinci sırada %27 ile yeteneğini kanıtlama dürtüsü gelmektedir [2].

İçeriden gelen saldırılar, çoğunlukla kurumların beklemedikleri ve hazırlıklı olmadıkları saldırılardır. Bu nedenle iç saldırıların belirlenmesi ve engellenmesi için daha az sayıda güvenlik önlemi bulunmaktadır. Veri koruma alışkanlıkları geliştirilmiş ve veri güvenliği politikası iyi düşünülmüş kurumlar, içeriden ya da dışarıdan gelen saldırılardan korunmak ve kurtulmak için diğer kurumlara göre daha iyi bir durumdadır. Bununla birlikte, birçok kurumda, çalışanlar veri korumasının öneminin farkında olduklarını söylemelerine karşın, günlük işlerin hızlı ve verimli bir şekilde gerçekleştirilmeye çalışılması nedeniyle, kurumun veri güvenliğinin sağlanması için atılan adımlar daha az önceliğe sahip olmaktadır.

İçeriden yapılan saldırıların belli bir kısmı kötü niyetli olmasına karşın bir kısmı bilinçsiz ve kasıtsız yapılan eylemlerdir. Clearswift Insider Threat Index tarafından (CITI) 2015 yılında yayımlanan rapora göre, güvenlik bozucu davranışların %67'sinin istemsizce ve yanlışlıkla yapılan davranışlardan, geriye kalan %33'ünün ise bilinçli ve kötü niyetli eylemlerden kaynaklandığı açıklanmaktadır [3].

Yukarıda belirtildiği gibi, içeriden yapılan saldırıların çoğunluğu bilgi sistemine erişim hakkı olan kişiler tarafından gerçekleştirilmektedir. Bu nedenle bazı kolaylıklara sahiptirler. Diğer taraftan bu durum bilgi güvenliği yöneticisinin işini zorlaştırmaktadır [4]. İçeriden yapılan saldırıların belirlenmesi amacıyla kurumsal ağ üzerinde giden bütün veri paketleri incelenmektedir. Gerçekleştirilen analiz türüne bağlı olarak, saldırı belirleme sistemleri imza temelli (kötüye kullanım amaçlı saldırıların belirlenmesi) veya olağan dışı durum temelli (olağan dışı saldırıların belirlenmesi) olarak sınıflandırılmaktadır. İmza temelli yaklaşım bilinen saldırıların belirlenmesinde kullanılırken; olağan dışı durum temelli yaklaşım olağan ağ davranışlarından farklılık gösteren davranışların belirlenmesinde kullanılmaktadır.

Bu çalışma, ağ davranış çözümlemesi yaklaşımı ile ağın olağan davranışlarının oluşturulmasını ve ağda meydana gelen farklılıkların belirlenmesini içermektedir.

1.1 Tezin Amacı

Bu tez kapsamında, kurum içi olası saldırılar incelenmekte ve alınabilecek önlemler açıklanmaktadır. Ayrıca ağ davranışı çözümlemesi yaklaşımı ile ağın olağan davranış modelinin oluşturulması ve ağ üzerinde oluşan olağan dışı durum ve saldırıların belirlenmesi amaçlanmaktadır.

1.2 Kaynak Araştırması

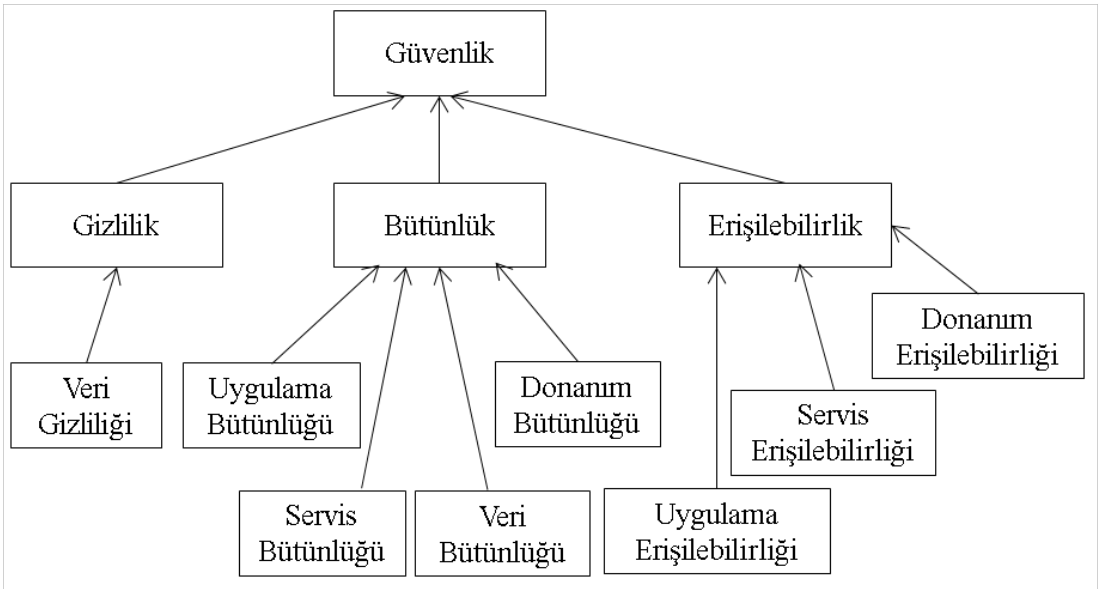
Bilgi güvenliği özellikle finans ve devlet kurumları gibi büyük kuruluşların çoğunda, giderek artan bir endişe kaynağı olmaktadır. Bilgi sistemlerinin giderek büyüyen karmaşık yapıları hem içerdikleri verilerin ve hem de kendilerinin korunmalarını daha zor hale getirmektedir. Tek bir korunmasızlık veya sistemin herhangi bir bileşeninde güvenlik açıklığı bulunması ciddi güvenlik sorunlarına yol açabilmektedir.

Güvenlik bozucu girişimlerin anlaşılması ve belirlenmesi kendi içerisinde birçok aşamayı içermektedir. Bu tez çalışması ile saldırıların nasıl yapıldığı ve saldırıların belirlenmesinde uygulanabilecek yöntemler inceleneceği için konuyla ilgili yapılan önceki çalışmalar güvenlik gereksinimlerinin çözümlenmesi ve saldırıların belirlenmesi biçiminde iki farklı başlık altında incelenmiştir.

1.2.1 Güvenlik Gereksinimlerinin Çözümlenmesi

Tanımlanmış saldırılar, güvenlik gereksinimlerinin temelini oluşturmaktadır. Bu nedenle sistemdeki olası saldırıların (tehditlerin) ortaya çıkarılması, güvenli sistemlerin oluşturulmasında kullanılan önemli bir adımdır.

İnsanlar, iş süreçleri, yazılım uygulamaları ve donanım bileşenlerinden oluşan düzenli sistemlerde (sosyo-teknik sistemler, STS) yer alan güvenlik bozucu olaylar büyük maddi zararlara neden olabilmektedir. Bu sistemlerdeki güvenliğin aşılabilmesinin en büyük nedeni ise sistemin bir bütün olarak değil aşama aşama tasarlanmasıdır [5]. Bu soruna ek olarak sistemin tasarımını yapan kişilerin sisteme yapılabilecek saldırılar hakkında yeterli bilgilerinin olmaması, durumu daha da kötüleştirmektedir [6]. Li ve Horkoff, çalışmalarında bu sorunu çözmek için, iş süreçleri, uygulamalar ve fiziksel altyapıyı içeren üç katmanlı bir güvenlik çözümleme sistemi önermektedir. Tasarlanan çözümleme sisteminde, üst seviye güvenlik gereksinimlerinden başlanarak, Şekil 1.1'de gösterilen güvenlik öznitelikleri çerçevesinde, her katman için gereksinimler belirlenmekte ve bu gereksinimlerin alt katmanları da kapsaması beklenmektedir. Böylece bütüncül bir güvenliğin sağlanması amaçlanmaktadır [5].



Şekil 1.1 : Güvenlik özniteliği hiyerarşisi.

Güvenlik gereksinimlerinin çözümlemesi sırasında karşıt hedef çözümlemesi [7] ve kötüye kullanım [8] yaklaşımları kullanılmaktadır. Ancak, bu yaklaşımlar yazılımlar için geliştirilmiştir. Bu nedenle çeşitli sistem bileşenleri (insanlar, yazılım, donanım vb.) arasındaki ilişkileri açıkça yakalayamamakta ve geçmişe yönelik saldırıları çözümleyememektedir. Bu soruna çözüm olarak, sistem güvenlik çözümlerini destekleyen, tekrarlanabilir saldırıları belgeleyen saldırı modelleri sunulmaktadır [9].

Saldırı modelleri, denenmiş saldırı bilgisini yeniden kullanmak amacıyla 2001 yılında ilk olarak Moore ve arkadaşları [10] tarafından önerilmiştir. Saldırı modelleri, sisteme zarar vermek isteyen saldırganın karşılaşabileceği zorlukları ve bunları çözmek için belirleyeceği stratejiyi tanımlamaktadır. Her saldırı modeli, bir saldırının belirli bölümlerinin nasıl tasarlandığı ve yürütüldüğü hakkında bilgi toplamakta ve saldırının etkinliğinin azaltılması konusunda yol göstermektedir [11].

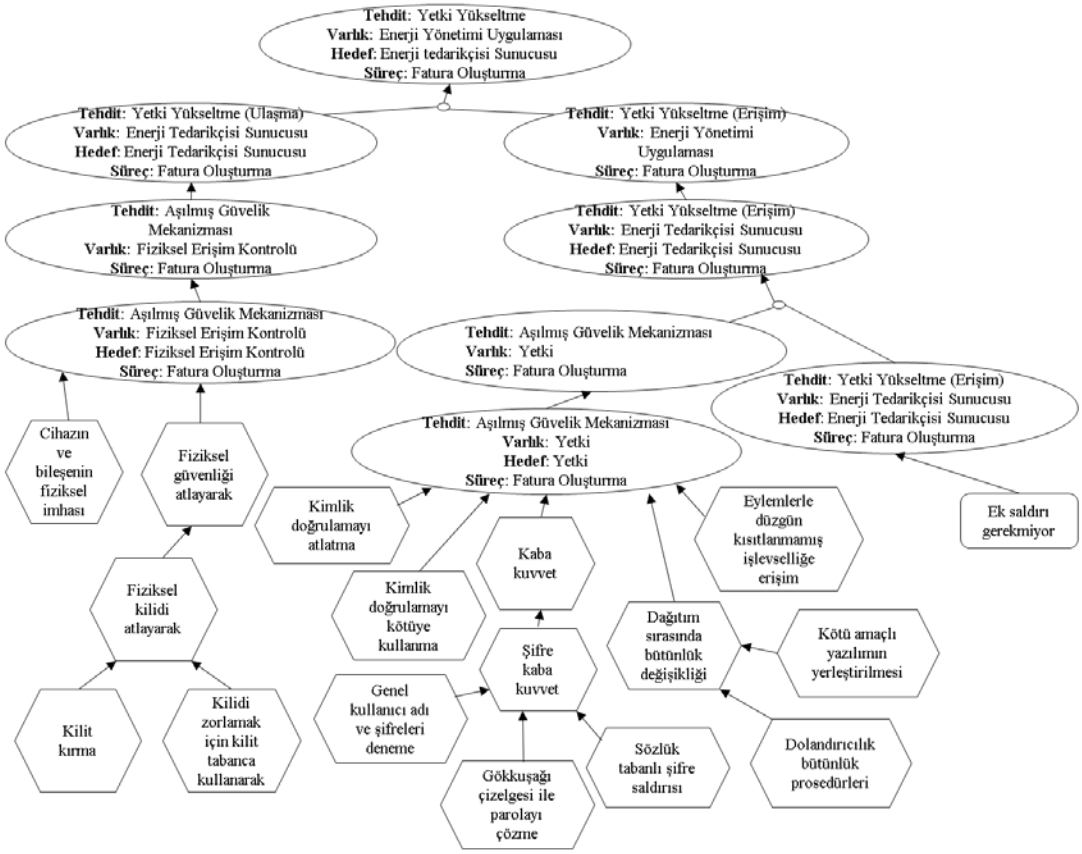
CAPEC [11], saldırganların uygulama ya da sistemdeki güvenlik açıklıklarını nasıl kullandığını anlamaya yardımcı olan 519 tane ortak saldırı modeli içermektedir. Li ve arkadaşlarının devam eden çalışmasında, CAPEC içerisinde yer alan saldırı modelleri incelenerek, saldırganın kötü niyetli ve çok aşamalı yaklaşımını çözümleyen yarı bağımsız ya da bağımsız güvenlik çözümleme tekniğinin geliştirilmesi amaçlanmıştır [12]. Bu kapsamda, yapılan saldırının, tanımlanmış saldırı modeli ile eşleşip eşleşmediği sınanmakta; eşleşmenin olmadığı durumlarda, (yeni durumun) saldırı olup olmadığı kararının güvenlik çözümleyici tarafından belirlenmesi ve yeni saldırı modelinin risk derecesi belirlenerek sisteme eklenmesi beklenmektedir [12] [13] [14].

Uygulanabilir saldırı stratejilerinin belirlenmesi, hedeflenen güvenlik çözümlemesi için önemli bir durumdur [14]. Saldırı senaryolarının düzenlenmesinde hedef modelleme tekniği [15] kullanılarak, sistematik olarak geliştirilebilir ve uygulanabilir somut saldırılar belirlenebilmektedir. Ayrıca güvenlik sorunlarını tanımlamak ve sınıflandırmak için Microsoft tarafından geliştirilen ve Çizelge 1.1 ’de gösterilen STRIDE saldırı modeli [16] kullanılabilmektedir.

Çizelge 1.1 : STRIDE tehdit modeli.

Saldırı		İstenen Özellik
Spoofing	Aldatma	Kimlik Denetleme
Tampering	Veri Değiştirme	Bütünlük
Repudiation	Reddetme	İnkar Edememe
Information Disclosure	Bilgilerin İfşası	Gizlilik
Denial of Service	Servis Engelleme	Erişilebilirlik
Elevation of Privilege	Yetki Yükseltme	Yetkilendirme

Şekil 1.2 ’de “Akıllı Sayaç Sisteminde” saldırganın, yetki yükseltmek için hedef alabileceği sistem varlıklarını ve saldırının gerçekleşme yollarını gösteren uygulanabilir saldırı modeli gösterilmektedir [14]. Model üzerinde saldırgan ilk olarak “maymuncuk (lock picking)” yöntemi ile enerji sağlayıcısının sunucusuna erişebilmekte ve erişim sağlandıktan sonra “gökkuşağı çizelgesi ile parolayı çözme (rainbow table password cracking)” yöntemi ile sunucu üzerinde yetki elde edebilmektedir.



Şekil 1.2 : Yetki yükseltme saldırısı için uygulanabilir saldırı modeli.

Güvenlik çözümleme sistemi, ağ ve güvenlik hakkında özellikle teknik bilgiye sahip olmayan kişilerin, sisteme yapılabilecek saldırıları belirleyebilme ve çözümleyebilmesi için temel oluşturmaktadır. Ayrıca kişilerin, saldırgan gibi düşünmesine, risklere odaklanmasına ve uygulamaya geçmeden önce güvenlik gereksinimlerinin iyi anlaşılmasına olanak tanımaktadır.

Korunması gereken varlıklar belirlendikten ve olabilecek saldırılar modellendikten sonra sistemin korunması için uygun önlemlerin alınması gerekmektedir. Bu kapsamda yapılan çalışmalar, saldırıların belirlenmesi başlığı altında açıklanmıştır.

1.2.2 Saldırıların Belirlenmesi

Saldırıyı belirleme, çok sayıda saldırının bilgisayarları sürekli olarak etkilemesi nedeniyle ağ yönetiminin en önemli bileşeni haline gelmiştir. Saldırı belirleme sistemleri virüs koruma yazılımları, güvenlik duvarları ve erişim denetimi kuralları gibi bilgi ve işletim sistemlerinin güvenliğinin güçlendirilmesi amacıyla kullanılmaktadır. Bu sistemler bilgisayar ağındaki ya da bilgisayar sistemindeki önemli noktalara dayanarak bilgi toplamakta ve güvenlik stratejisine aykırı bir durum olup olmadığını ya da ağ veya sistem üzerinde saldırı belirtilerinin olup olmadığını incelemektedir.

Kabiri ve Ghorbani (2005) [17] ve Sobh (2006) [18] tarafından yapılan araştırmalarda da gösterildiği gibi, birçok saldırı belirleme sistemi önerilmektedir. Ancak bu teknolojinin başlangıcı Denning (1987) [19] ve Staniford-Chen ve arkadaşları (1998) [20] tarafından yapılan çalışmalar ile ilişkilendirilmektedir.

Bu konu ile ilgili en dikkate değer çalışmalar, temel olarak Sızmanın Algılanması (Intrusion Detection System: IDS) alanında ortak bir çerçevenin düzenlenmesi ve tanımlanması yönünde, 1998 yılında DARPA (Defence Advanced Research Project Agency) tarafından kurulan CIDF (Common Intrusion Detection Framework) isimli takım tarafından başlatılmıştır. Çalışmalar dört farklı işlevsel modülü temel alarak genel bir IDS mimarisi tasarlayan ve 2000 yılında IETF (Internet Engineering Task Force) bünyesinde oluşturulan IDWG (Intrusion Detection Working Group) isimli çalışma takımı tarafından yürütülmüştür [21].

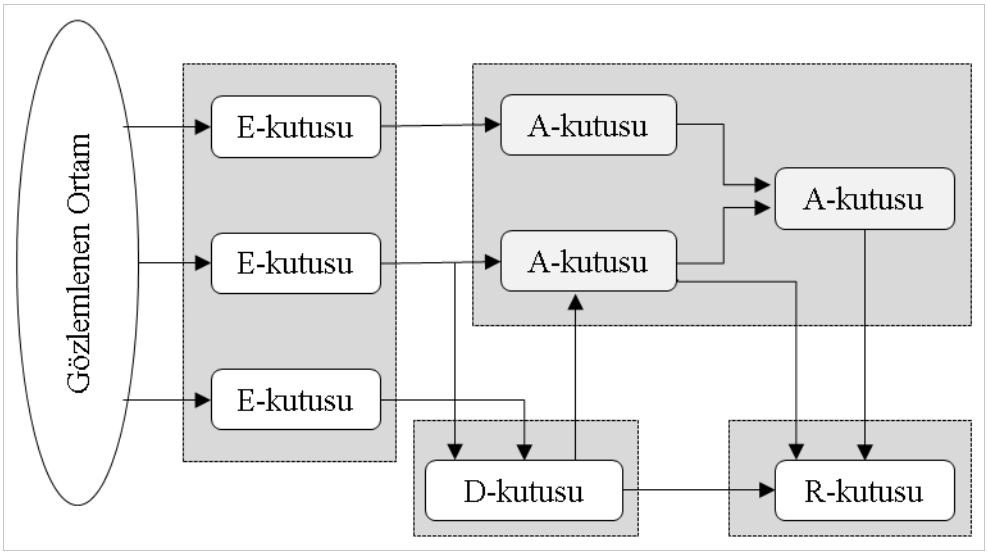
CIDF'in ana çalışma konusu IDS'in sistem yapısı, iletişim sistemi, tasarım dili ve API (Application Programming Interface) olarak dört bölümden oluşmaktadır. CIDF tarafından tasarlanmış saldırı belirleme sisteminin ana yapısı Şekil 1.3 ’te gösterildiği gibi dört temel bileşenden oluşmaktadır [22]. Bu bileşenler aşağıda açıklanmıştır:

E blokları (Olay-kutucukları): Hedef sistemi izleyen duyarga bloklarıdır. Bu blok tarafından elde edilen bilgiler diğer bloklar tarafından çözümlenmektedir.

D blokları (Veri tabanı-kutucukları): E bloklarından elde edilen verilerin depolandığı saklama alanlarıdır. Burada depolanan veriler sonraki işlemlerde A ve R blokları tarafından kullanılmaktadır.

A blokları (Çözümleme-kutucukları): Olayların çözümlenmesi ve olası düşmanca davranışların belirlenmesi için kullanılan işlem modülleridir. Ayrıca gerekli olduğu durumlarda alarm üretmektedirler.

R blokları (Tepki-kutucukları): Belirlenen olası saldırının engellenmesi için bir yanıtın oluşturulmasında kullanılmaktadır.



Şekil 1.3 : CIDF tarafından oluşturulan ortak çerçeve.

IDGW saldırı belirleme çalışma takımı, IDS bileşenlerinin kendi aralarında iletişim kurabilmesi için nesne yönelimli düşünceyi benimseyerek saldırı belirleme değişim protokolünü (IDXP, RFC 4767) [23] ve XML temelli saldırı belirleme mesaj değişim formatını (IDMEF, RFC 4765) [24] hazırlamıştır. Böylece belirlenen ortak protokoller ile iletişim sorunsuz sağlanmaktadır. Bunu dışında, IDGW, üretilen alarmların saldırı belirleme sistemi içinde dağıtılmasını sağlayan saldırı alarm protokolünü (IAP) [25] hazırlamıştır. IAP, TCP'nin üzerinde çalışan bir uygulama katmanı protokolüdür. HTTP protokolü temel alınarak tasarlanmasına karşın üzerine herhangi bir uçtan bağlantı başlatma, şifreleme ve kimlik doğrulama ile birleştirilme gibi özellikler de eklenmiştir [22].

Ele alınan bilgi kaynağına bağlı olarak (Şekil 1.3 : E blokları) saldırı belirleme sistemleri sunucu ve ağ temelli olarak ayırılmaktadır. Sunucu temelli sistemler temel olarak işletim sistemiyle ilgili süreç tanımlayıcıları ve sistem çağrıları gibi olayları incelerken; ağ temelli sistemler trafik hacmi, IP adresleri, kullanılan protokoller gibi ağla ilişkili olayları incelemektedir.

Gerçekleştirilen analiz tipine bağlı olarak (Şekil 1.3 : A blokları), saldırı belirleme sistemleri imza temelli (kötüye kullanım temelli) veya olağan dışı durum temelli olarak sınıflandırılmaktadır. İmza temelli sistemler bilinen saldırıları bir veri tabanında saklamakta ve bu veri tabanını kullanarak saldırıları belirlemektedir. Olağan dışı durum temelli sistemler ise korunacak sistemin olağan davranışını öngörmeye çalışmakta ve belirli bir andaki gözlem ile olağan davranış arasındaki sapmayı karşılaştırmaktadır. Sapmanın belirlenmiş eşiği aşması durumunda ise alarm üretilmektedir.

Kaynaklarda bu yöntemleri temel alarak saldırı belirleme sistemlerini geliştirmeye yönelik çalışmalar yer almaktadır. Aşağıda bu çalışmalardan bazıları anlatılmıştır:

Tlyman [26] çalışmasında, bilgisayar ağlarında saldırıyı belirleme için, Snort ve NIDS'in çalışma mantığını kullanarak yeni işlem aşamaları eklenmiş Bayes ağları uygulamasını sunmaktadır. Sunulan bu çözüm hem kötüye kullanım temelli hem de olağan dışı durum temelli saldırı belirleme için kullanılabilir olmasına karşın saldırı belirleme oranının arttırılması ve üretilen yanlış alarmların azaltılması amacıyla kötüye kullanım temelli yöntem yeğlenmiştir.

Vilar ve arkadaşları [27], çalışmalarında sürekli ve anlık saldırıların belirlenmesinde Makine Öğrenmesi (ML) ya da Yapay Zeka (AI) tekniklerinin kullanılarak gerçekleştirilmesi için çok yüksek işlem başarımı gerektirdiğinden bahsetmektedir. Bu nedenle “Timed Observation” isimli bir kuram üretilerek olasılık yaklaşımından çok başarımı arttırılmış denetim bloklu (kural temelli) yapı önerilmektedir. Çalışmada genel olarak, müşteri farklı hesaplara para aktarımı yaptığında banka yöneticisinin bundan faydalanamaması hedeflenmiştir. Bu kapsamda işlemlerin, zaman diyagramı kullanılarak karşılaştırılması yöntemi izlenmiştir.

Geleneksel saldırı belirleme sistemleri, bilinen saldırılar için koruma oluşturmasına karşın kötü niyetli davranışları çoğunlukla belirleyememekte ve yanlış alarmların üretilmesine neden olmaktadır. Böyle durumlarda ağ güvenlik yöneticinin saldırı belirleme sürecine müdahale etmesi gerekmekte ve saldırının işaretlenerek sisteme elle eklenmesi gerekmektedir. Bu soruna çözüm olarak, uzman müdahalesini azaltarak sistemi daha otomatik hale getiren ve kötü niyetli davranışları belirleyebilen ağ davranış çözümlemesi, veri madenciliği yöntemleri ve makine öğrenmesi teknikleri sunulmaktadır.

Kakuru [28] çalışmasında içeriden yapılan etkin ya da edilgen saldırıların belirlenmesinde kullanılacak, işletim sisteminden bağımsız bir davranış çözümleme aracının geliştirilmesine odaklanmıştır. Desen eşleştirme yöntemini temel almakta olan bu uygulama temel olarak kullanıcıların davranışlarına ilişkin istatistiksel verilerin ve ağ trafiğinin ayrıntılı çözümlenmesinin sonucu olan modellere dayanmaktadır. Oluşturulan ağ modelleri, trafiği çözümleme aracının geliştirilmesinde kullanılmaktadır.

Çalışmanın amacı, kurum ağında yer alan yetkili kullanıcıların olağan olmayan davranışlarının belirlenmesidir. Bu kapsamda Ağ Davranışını Çözümleme (Network Behaviour Analysis – NBA) yöntemi kullanılmıştır. Bu yöntem iki adımı içermektedir. Birinci adımda kullanıcının ağ ile olan etkileşimi belli bir süre boyunca izlenerek kayıt edilmektedir. Ağ trafiğini kayıt altına almak için paket dinleyicisi (wireshark ve tcpdump programları) kullanılmıştır. İkinci adımda ise kullanıcının o andaki davranışı ile geçmiş davranışları karşılaştırılarak eşleşme araştırması yapılmaktadır. Eşleşmenin olmadığı durumlarda yeni bir davranışın sergilendiği belirtilmekte ve güvenlik yöneticisine uyarı bilgisi gönderilmektedir.

Çalışmanın akışı şöyledir: İlk aşamada kullanıcının eriştiği web sayfaların dökümü alınmaktadır. Bu dökümden sayfalara ilişkin kaynak IP adresi, hedef IP adresi, kaynak MAC adresi, hedef MAC adresi, DNS protokolü, zaman, paket numarası ve sunucu ismi bilgileri elde edilmektedir. İkinci aşamada, veri tabanı kısmı düzenlenmektedir. Veri tabanı içerisinde kullanıcı bilgilerini, web sayfalarına ilişkin bilgileri ve tüm kullanıcıların web siteleri desenini içeren 3 tablo tutulmaktadır. Erişim izni olmayan kullanıcı bir siteye erişmeye çalıştığı an uyarı üretilmekte ve güvenlik yöneticisine bildirilmektedir. Güvenlik yöneticisi, bu davranışı onaylarsa, kullanıcı işleme devam edebilmekte ve davranış kaydedilmektedir aksi durumda kullanıcı erişim sağlayamamaktadır. Geliştirilen uygulama kullanıcının davranışları üzerinde çalıştığı için, kullanıcı kendi bilgisayarını değiştirdiğinde ve farklı bir bilgisayarda çalıştığında ağ yöneticisi kullanıcıyı tanımlayabilmektedir.

Bu çalışma, davranış modellerinin anlaşılması için temel seviyede örnek alınabilir. Ancak günümüz gelişmiş sistemleri için yeterli değildir.

Han ve Kim [29] çalışmalarında sıfır gün saldırılarına karşı tek çözümün bilinen saldırılara bağımlı olan imza temelli saldırı belirleme yönteminden çok olağan dışı durum temelli saldırı belirleme yönteminin kullanılması olduğunu belirtmektedir. Olağan dışı durum temelli yöntemde, olağan durum örüntüsü belirlenerek olağan dışı durumlar belirlenmeye çalışılmaktadır. Bu çalışmada ise tam tersi bir yaklaşım izlenerek olağan dışı durumların örüntüsü çıkarılmaktadır. Bu kapsamda, kötü amaçlı yazılımlar kullanılarak ağ akışı izlenmekte ve işlem zamanı, kaynak IP adresi, hedef IP adresi, kaynak iskele numarası, hedef iskele numarası gibi bilgiler depolanmaktadır. Depolanan bu veriler k-ortalama algoritması kullanılarak kümeleme işlemi gerçekleştirilmiş ve model oluşturulmuştur. Böylece gözlemlenmeye devam edilen ağ akışı kümelenmiş modele uyuyorsa saldırı, uymuyorsa normal davranış olarak tanımlanmaktadır.

Bu çalışma saldırı tespiti için farklı bir bakış sunmasına karşın bütün olası saldırıların izlenmesi ve önceden tekrar edilmesi olanaksız olacağı için saldırıları olağan davranış olarak tanımlama olasılığı çok yüksek bir yaklaşımdır.

Garcia [30] çalışmasında eskiden botnet'lerin daha basit yapıda olduğunu ve tek bir sahip tarafından yönetilerek aynı işin yaptırıldığını şimdi ise her botnet'in farklı görevleri üstlenerek saldırıların daha karmaşık hale geldiğini söylemektedir.

Çalışma da bilinen kötü amaçlı yazılımların statik parmak izleri, beyaz ve kara listeler, yığın kaynaklı tehdit istihbaratı çözümlemesi gibi çözümlerle gerçek zamanlı olarak belirlenebildiğini ancak bilinmeyen kötü amaçlı yazılımların belirlenemediğini açıklamaktadır. Bu soruna çözüm olarak kötü amaçlı yazılımların ağa etkisini çözümleyerek ağın davranış modelinin çıkarılması önerilmiştir. Bu kapsamda ağ akışında yer alan statik veriler dışında akışta yer alan paketlerin birbiri ile olan ilişkisine de bakılarak bir davranış modeli oluşturulmuştur. Davranış modeli oluşturulurken komuta kontrol kanalları üzerinde durulmuş ve Markov zincir temelli makine öğrenmesi algoritması kullanılmıştır. Oluşturulan model, benzer ağ trafiğinin oluşup oluşmadığının kontrolünde kullanılmaktadır.

Saldırılar her geçen gün daha karmaşık hale geldiği ve tespit edilmesi zorlaştığı için bu kapsamda yapılan çözümlemeler ve çalışmalar hızla devam etmektedir.

1.3 Tezin Katkısı

Günümüzde dışarıdan yapılan saldırlar için pek çok araştırma yapılmasına ve ürün geliştirilmesine rağmen içeriden yapılabilecek saldırıların önemi son dönemde ortaya çıkmıştır. Bu kapsamda kurum ya da kuruluş içerisinde oluşabilecek saldırı türleri ve açıklıklar incelenerek alınabilecek önlemler hakkında açıklamalar yapılmıştır.

Bu çalışma, kurum ya da kuruluş içinde çalışan kullanıcıların ağ üzerindeki davranışlarını inceleyerek, ağ üzerinde oluşan yeni ve olağan dışı durumların belirlenebilmesi için derin öğrenme yaklaşımının temelini oluşturan yapay sinir ağları algoritmasını kullanarak modelleyen bir yapı geliştirmeyi amaçlamaktadır.

1.4 Tezin Düzeni

Giriş bölümünde tezin genel kapsam ve amaçları tanımlanmaktadır. Ayrıca konuyla ilgili yapılmış güncel çalışmalar özetlenmekte ve tezin katkısı belirtilmektedir.

Saldırılar ve Güvenlik Açıklıkları bölümünde kurum ya da kuruluş içinde yapılabilecek saldırıların tanımı verilmekte ve alınabilecek stratejik ve sistemsel önlemler açıklanmaktadır.

Saldırı Belirleme Yöntemleri bölümünde sisteme yapılabilecek saldırıların belirlenmesinde kullanılan yöntemler açıklanmaktadır.

Geliştirilen Yöntem bölümünde ağ modelinin oluşturulması ve olağan olmayan davranışların belirlenmesi kapsamında geliştirilen yöntem anlatılmaktadır.

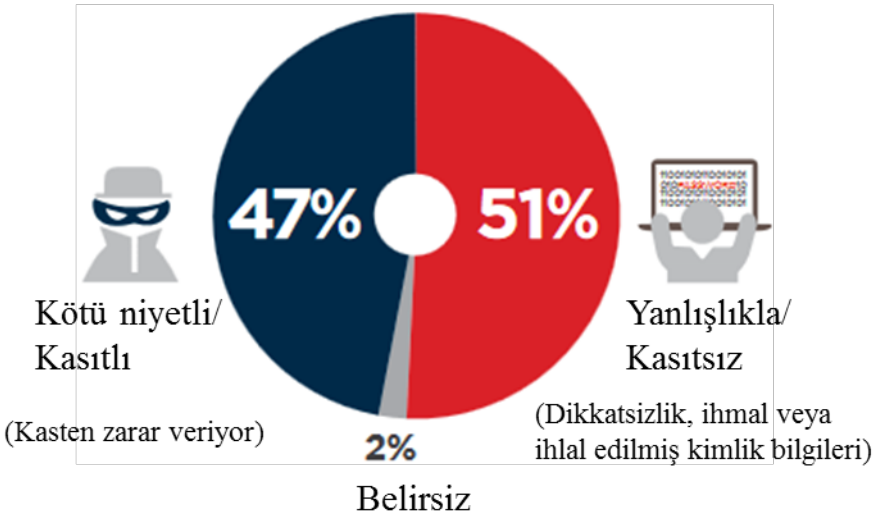
Sonuç ve Öneriler bölümünde çalışma sonucunda elde edilen veriler paylaşılmakta ve gelecekte yapılabilecek çalışmalar hakkında bilgi verilmektedir.

2. SALDIRILAR VE GÜVENLİK AÇIKLIKLARI

İç saldırılar bir ağa ya da bilgisayar sistemlerine yetkili erişime sahip kişiler tarafından yapılan güvenlik ihlalleri olarak tanımlanmaktadır. Kurum içinde bulunan kişilerin, kurumun politikalarını, güvenlik süreçlerini ve teknolojisini iyi bilmesi dış saldırganlara göre önemli bir üstünlük sağlamaktadır. Bununla birlikte kurumun güvenlik açıklıklarının farkında olan kişiler bilgi güvenliği kapsamında daha fazla risk oluşturmaktadır. İç saldırıyı yapabilecek kötü niyetli kişiler, kurumun güvenlik önlemlerini düzenleyen veya yöneten kişilerden de oluşabilmektedir.

Bununla birlikte diğer önemli bir nokta ise, son dönemlere kadar birçok kurumun içeriden oluşabilecek tehditlerin veya saldırıların farkında olmaması nedeniyle çoğunlukla dış saldırılara odaklanılmasıdır. Bu nedenden dolayı da iç saldırılar için daha az güvenlik önlemi bulunmaktaydı. İç saldırıların daha maliyetli ve tehlikeli olması nedeniyle bu bakış açısının son yıllarda değiştiği görülmektedir.

Siber güvenlikte iç tehditler kavramı çoğu zaman kuruma hırsızlık veya sabotaj yoluyla doğrudan zarar vermek isteyen kötü niyetli çalışanlarla ilişkilendirilmektedir. Ancak çalışanların veya yüklenicilerin özen göstermemesi de istemeden çok fazla güvenlik ihlaline neden olmaktadır. CA Technologies tarafından yayımlanan İç Tehditler 2018 raporuna [31] göre kurumların, kullanıcı dikkatsizliği nedeniyle yanlışlıkla oluşan ve istenmeyen veri ihlalleri (%51) ve kötü niyetli kullanıcıların bilinçli neden olduğu güvenlik ihlalleri (%47) için eşit derecede endişeli oldukları belirtilmektedir (Şekil 2.1).



Şekil 2.1 : İç tehdit türleri.

İç tehditlerin ya da saldırılarının ne olduğunun ve nasıl oluştuğunun anlaşılması, bu saldırılardan korunmak için alınabilecek önlemlerin belirlenmesine ve hazırlanmasına yardımcı olmaktadır.

Kurum ya da kuruluş içerisindeki saldırılar genellikle çalışanlar, aday çalışanlar, öğrenciler ya da paydaşlar tarafından gerçekleştirilmektedir. Oluşan bu saldırıların nedeni benzer şekilde farklılık gösterebilmektedir ve bazı durumlarda saldırı teriminin kullanılması gerçekleştirilen eylemler için fazla ağır olabilmektedir. Bu gibi durumlar şu şekilde ifade edilmiştir [32]:

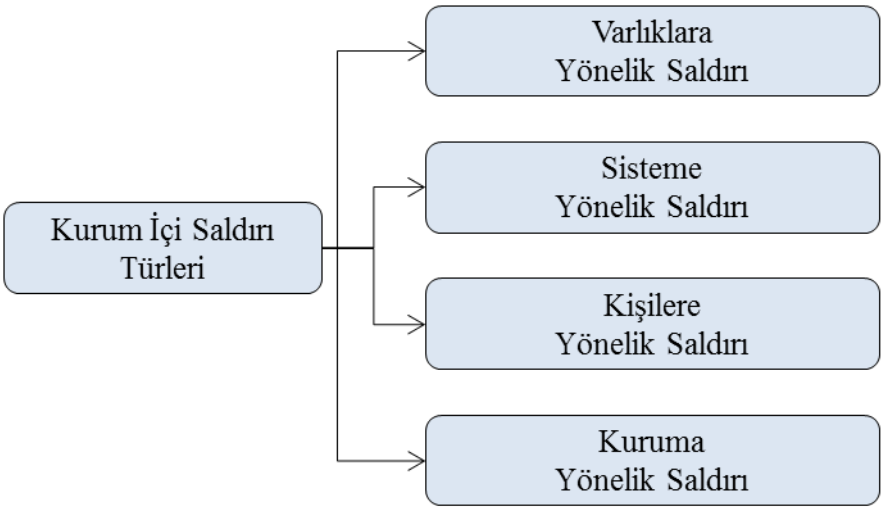
- İstemsiz yapılan hatalar.
- Gerekli görevleri yerine getirmeye çalışırken oluşan durumlar: Örneğin, sistemin desteklemediği bir eylemi yapmaya çalıştığı ya da yetkisiz olduğu bir bilgiyi kullanmaya çalıştığı ancak engellendiği durumlarda aynı görevi yapabilmek için dolaylı ve geçici çözümlerin denenmesi.
- Sistemin daha kullanışlı veya kullanılabilir hale getirilmesi amacıyla yenilikçi bir yaklaşım denenerek sistemin tasarlanmadığı bir şey yapmasını sağlamaya çalışmak.
- Sorunların belirlenmesi ve raporlanması amacıyla sistemin açıklıklarının araştırılması.
- Zaman öldürmek için verilerin görüntülenmesi.

- Yetki sınırlarının sınanması: Raporlama niyeti olmadan sistemin hata ve açıklıklarının araştırılması.

İç saldırılardan korunmanın ilk adımı kurum veya kuruluşlara ilişkin varlıkların ve bu varlıkları korumak için hangi kontrollerin mevcut olduğunun belirlenmesi ve sınıflandırılmasıdır. Bu kapsamda saldırı türleri başlığı altında kurum ya da kuruluşlara yapılabilecek saldırılar ve korunmaları için alınabilecek güvenlik önlemleri anlatılmaktadır.

2.1 Siber Güvenlik Saldırı Türleri

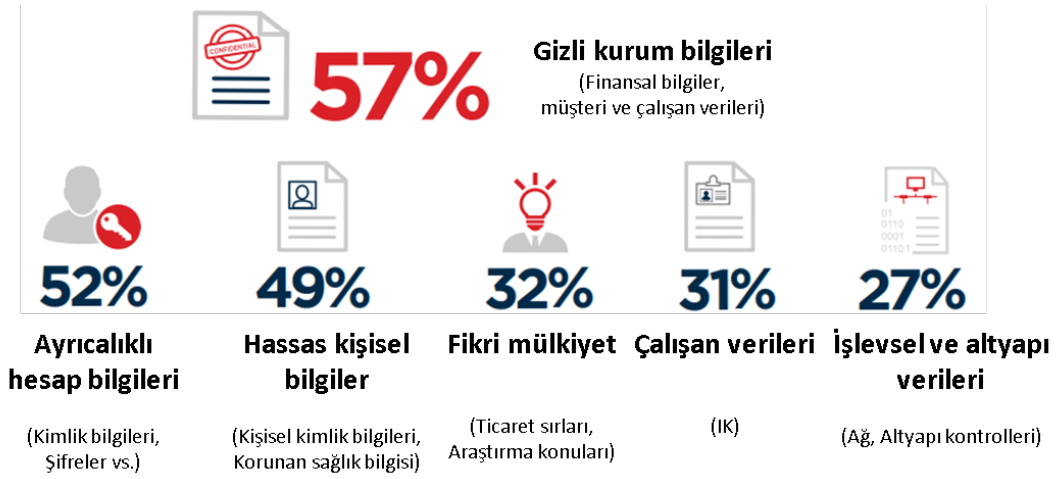
İçeriden yapılan saldırılar, kurum ya da kuruluşların sahip oldukları varlık, ürün ya da süreçlerine farklı şekillerde zarar verebilmektedir. Şekil 2.2 ’de içeriden yapılan saldırıların kurum içinde kimlere ya da nelere yönelik olabileceği gösterilmektedir.



Şekil 2.2 : Kurum içi saldırı türleri.

2.1.1 Varlıklara yönelik saldırılar

Veri sadece bilgi teknolojilerine ilişkin bir varlık olmaktan çıkarak bazı türleri diğerlerinden daha değerli olan temel stratejik bir varlık konumuna gelmiştir. Kurumların finansal bilgileri, müşteri ve çalışan bilgileri gibi gizli ticari bilgiler yüksek değerli bir hedef olarak görülmektedir. Şekil 2.3’te saldırılara karşı korunmasız olan veriler gösterilmektedir [31].



Şekil 2.3 : İç saldırılar için savunmasız veri türleri.

Varlıkların türleri, korunma yöntemlerinde farklılıkların oluşmasına neden olmaktadır. Örneğin bir kurumun en değerli varlığının para olması durumunda bu varlığın fiziksel konumu, fiziksel olarak nasıl erişildiği ve korunduğu, kimin koruduğu, miktarının ne kadar olduğu ve nasıl kayıt altında tutulduğu, değişikliklerin nasıl engellendiği dikkat edilmesi gereken konular arasındadır. Diğer yandan en önemli varlığın veri olması durumunda, verinin hangi biçimde saklandığı (elektronik ya da fiziksel), saklanma biçimine göre nerede tutulduğu (sunucu ya da dosya dolabında), nasıl erişildiği (ağ üzerinden ya da fiziksel olarak dosya dolabını açarak), kimler tarafından erişildiği, değişikliklerin nasıl kayıt altına alındığı ve güvenlik kontrollerinin nasıl yapıldığı (kullanıcı adı – şifre ya da dolap kilidi) incelenmesi ve dikkat edilmesi gereken konular arasında yer almaktadır.

Verilere yönelik saldırılar, genellikle erişim yetkisi kısıtlı olan ya da tamamen engellenmiş verilerin gizliliğinin ihlal edilerek görüntülenmesi veya yetkili ya da yetkisiz olduğu verilerin içeriğinin uygun olmayan şekilde değiştirilmesidir.

Veri gizliliğinin ve bütünlüğünün ihlal edilmesi kapsamında aşağıdaki gibi saldırılar yapılabilmektedir.

Paket Dinleme: Bilgisayarlar arasında transfer edilen bilgilerin yakalanmasına yönelik ağın dinlenmesidir. Bu saldırı türünde, sistem üzerinde özellikle en basit ağ cihazlarından olan HUB kullanıldığında iletilmek istenen paket bütün portlara gönderildiği için ağ dinlemelerine karşı son derece zayıftır. Bu sebeple HUB yerine switch cihazlarının kullanımı tercih edilmeli ve aynı görevi yapan bilgisayarların aynı VLAN içinde toplanması gerekmektedir. Diğer bir koruma yöntemi ise verinin şifrelenerek gönderilmesidir. Böylece veriye erişim sağlanmış olsa bile içerik görüntülenememektedir.

Port Taraması: Saldırganın TCP / UDP bağlantı noktalarını tarayarak hedef bilgisayarda çalışan hizmetleri bulmaya çalıştığı bir ağ saldırısı türüdür. Açık bağlantı noktaları bulunduğunda hedef sistem üzerinde çalışan servis ve yazılım ürünleri tespit edilebilmektedir.

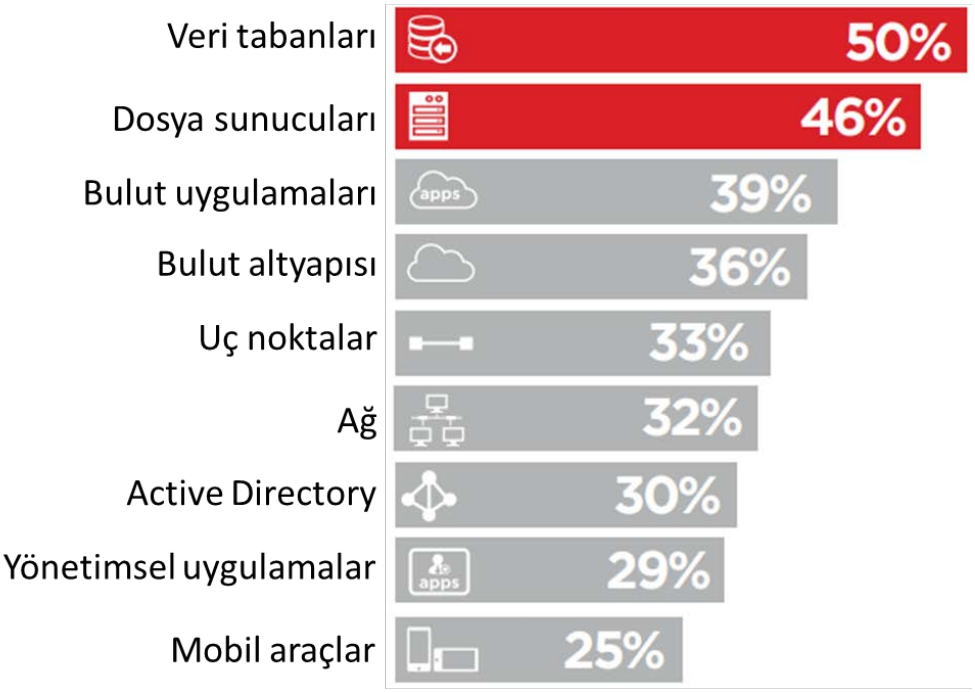
Salam Dilimi: Bir dizi küçük veri güvenliği saldırısının bir araya gelerek daha büyük bir saldırıya yol açan saldırı türüdür. Banka hesaplarından küçük miktarlarda paranın çalınması bu saldırı türüne örnek olarak verilebilmektedir.

Verinin Kurcalanması: Verilerin yasadışı ya da yetkisiz olarak değiştirilmesidir. Örneğin hesap yöneticilerinin, çalışan zaman çizelgesine ilişkin bilgileri maaş bordrosuna yansıtmadan değiştirmeleri verinin bütünlüğünü bozmaktadır.

2.1.2 Sisteme yönelik saldırılar

Sistemin devamlı erişilebilir olması kurumların günlük süreçlerin aksamadan işletilebilmesi için en önemli konulardan birisidir.

Şekil 2.4’de kurumdaki bilgi sistemlerinin iç saldırılara karşı korunmasızlık oranlarını göstermektedir [31].



Şekil 2.4 : Bilgi sistemlerinin korunmasızlık oranı.

Sisteme yönelik gerçekleştirilebilecek saldırılar aşağıdaki gibi açıklanmaktadır.

Fiziksel Tehditler: İstikrarsız güç kaynağı ve ani gerilim yükselmesi gibi elektrik güç sorunları ya da yangın ve sunucu odalarının nemlenmesi gibi donanımları yıpratıcı fiziksel tehditler sistemin erişilebilirliğini engelleyebilmektedir. Ayrıca sunucu odalarına giriş hakkına sahip kişilerin belirlenmesi ve denetlenmesi de fiziksel güvenlik için önemli bir yaklaşımdır.

Virüs - Solucan: Virüsler bilgisayarların çalışma düzenini bozan ve işlevselliğini engelleyen zararlı yazılımlardır. Virüslerin yayılabilmesi için bir kullanıcı tarafından tetiklenmesi gerekmektedir. Solucanlar da virüsler gibi sistemin işlevselliğinin bozulması için tasarlanmış yazılım türüdür. Virüsten farkı ise solucanlar kendi kendilerine çoğalma özelliğine sahiptirler.

Aldatma Saldırıları: Aldatma saldırılarından birisi MAC ve IP bilgilerinin eşleştirilerek tutulduğu ARP tablosunun bozulmasıdır. ARP zehirlenmesi olarak adlandırılan saldırıda, saldırgan aradaki adam yaklaşımını kullanarak hedef bilgisayarın tablosuna kendi MAC adresini "Ağ Cihazı MAC Adresi" olarak, ağ cihazı tablosuna ise "Hedef Bilgisayar MAC Adresi" olarak tanıtarak ağ trafiğinin kendisi üzerinden geçmesini sağlamaktadır.

Diğer bir aldatma saldırısı ise bilgisayarlara ilişkin MAC adreslerinin değiştirilmesidir. Bilgisayarlar ilk üretildiğinde MAC adresi sabit olarak verilmekte ve bu MAC adresi bilgisayarın kimliğini ifade etmektedir. Ancak bazı uygulamalar ile bu MAC adresi değiştirilebilmektedir. Böylece bir ağdaki bir bilgisayarı gizleyerek veya başka bir ağ aygıtının kimliğine bürünerek sunucu ya da yönlendiriciler üzerindeki erişim kontrol listelerinin aşılması istenmektedir.

Şifre Ele Geçirme: Bu saldırı türünde hedef bilgisayara erişim elde edilmesi amacıyla yetkili bir kullanıcının parolası ele geçirilmeye çalışılmaktadır. Genel olarak bu amaç için şifre kombinasyonlarını deneyen zorlama ya da genel kullanılan şifreleri içeren sözlük saldırısı kullanılmaktadır. Bu saldırılardan korunmak amacıyla kurum ya da kuruluşlarda kullanıcıların kimliğini doğrulamak ve yetkilendirmek için yaygın olarak kullanılan LDAP (Lightweight Directory Access Protocol), RADIUS (Remote Authentication Dial-In User Service) ya da Microsoft Active Directory sistemleri kullanılmaktadır.

2.1.3 Kişilere yönelik saldırılar

Kişilere yönelik saldırılar, kurum içinde çalışan kötü niyetli bir kişinin diğer çalışanlara, eski çalışanlara ya da müşterilere yönelik gerçekleştirmiş olduğu saldırı şeklidir.

2.1.3.1 Çalışana yönelik saldırılar

Kurum ya da kuruluş içinde çalışan bir kişinin başka bir çalışana yapmış olduğu saldırı türüdür. Bu saldırı türü genellikle sosyal mühendislik saldırılarını kapsamaktadır. Sosyal mühendislik çeşitli kötü amaçlı eylemlerin insan etkileşimleri yoluyla gerçekleştirilmesidir. Bu kapsamda güvenlik hatalarının yapılması veya hassas bilgilerin paylaşılması için kullanıcılar kandırılmaya çalışılmaktadır. Böylece zayıf güvenlik protokollerini öğrenebilmekte, bir kullanıcının kullanıcı adı ve şifresi ele geçirebilmekte ya da yetkisiz olduğu bir odaya girebilmektedir.

Bu saldırılar tamamen yetkili kişiler tarafından bilerek ve isteyerek yapılan hatalar olduğu için tespit edilmesi çok zordur. Bu sebeple sosyal mühendislik saldırılarından korunmanın en iyi yolu kurum içinde çalışanların eğitilmesi ve düzenli hatırlatmaların yapılmasıdır.

2.1.3.2 Müşteriye yönelik saldırılar

Müşteriye yönelik saldırılar, kurum ya da kuruluşların kendi müşterilerine yapmış oldukları saldırı türüdür. Bu saldırının en güncel örneği 2018 yılında Facebook sosyal medya uygulamasını kullanan bütün kullanıcıların kişisel bilgilerinin kötü niyetli kurumlara satılmasıdır.

2.1.4 Kuruma yönelik saldırılar

Kurum ya da kuruluşa yönelik saldırılar doğrudan kuruma zarar verici davranışları içermektedir. Bu davranışlar, kurumun finansal olanaklarının kullanılmasına yönelik ya da kurumun adını kötülemeye yönelik olabilmektedir. Örneğin banka müşterisine haksız kredi verilmesi, kara para aklama, tedarik dolandırıcılığı ya da güvenlik politikalarının ihlali kuruma yönelik saldırılardan bazılarıdır.

2.2 Güvenlik Açıklıkları

Yazılım kodunda ya da sistemin herhangi bir yerinde oluşan hatalar virüs, solucan, Truva atı gibi zararlı yazılımların ya da yetkisiz bir kişinin istismar edebileceği güvenlik açıklıklarının oluşmasına neden olabilmektedir. Güvenlik açıklıkları bilinçli ya da bilinçsiz olarak meydana gelebilmektedir.

2.2.1 Bilinçli açıklıklar

Bilinçli açıklıklar, sistemin geleneksel güvenlik mekanizmalarını atlayarak bilgisayar sistemine veya şifrelenmiş verilere saldırı yapılması amacıyla oluşturulan arka kapılardır.

2.2.2 Bilinçsiz açıklıklar

Bilinçsiz açıklıklar kurum ya da kuruluş içinde kullanılan yazılımlardan, işletim sistemlerinden ya da kişiler tarafından oluşturulabilmektedir.

2.2.2.1 Sistem açıklıkları

Sistem açıklıkları kullanılan uygulamalardan ya da işletim sistemlerinden kaynaklı oluşabilen güvenlik zayıflıklarıdır. 1998 yılından bugüne kadar bulunan işletim sistemleri açıklıkları CVE (Common Vulnerabilities and Exposures)'nin [33] sitesinde güncel olarak yayınlanmaktadır.

Son yılların en çok duyulan saldırısı 2017 yılında gerçekleştirilen ve Windows işletim sistemlerini hedef alan WannaCry ransomware zararlı yazılımıdır. Bu saldırı SMB (Server Message Block) portundaki açıklığı kullanarak sistemdeki verileri şifrelemekte ve şifrenin kaldırılması için fidye ödemesi talep etmektedir.

2.2.2.2 Çalışan hatası

Çalışan hataları kurum ya da kuruluş içinde çok ciddi açıklıkların oluşmasına neden olabilmektedir. Kurum içindeki haberleşme ağının SSH şifreli ağ yerine Telnet açık ağ üzerinde oluşturulması, erişim yetkilerinin düzgün tanımlanmaması ve gerekli sıklıkta güncellenmemesi, hassas verilerin güvenliği sağlanmış bir sunucu yerine kullanıcı makineleri üzerinde tutulması, kullanıcıların çok basit düzeyde ya da tahmin edilebilir şifreler oluşturması gibi hatalar saldırıların kolayca gerçekleşmesine neden olabilmektedir. Bu hataların azaltılması için çalışanların güvenlik konusunda eğitilmesi gerekmektedir.

3. SALDIRI BELİRLEME YÖNTEMLERİ

Bu bölümde, bilgi sistemine yapılabilecek saldırıların belirlenmesinde kullanılan güncel ve geçerli yöntemler açıklanmaktadır.

Genelağ ve bilgisayar ağları her geçen gün artan sayıda güvenlik saldırısıyla karşılaşmaktadır. Sürekli olarak yeni tür saldırıların ortaya çıkması, güvenlik sağlayıcı çözümlerin daha esnek, uyarlanabilir olmasını gerektirmektedir. Bu bağlamda, hedef sistemlerin ve ağların zararlı saldırılara karşı korunmasında, imza temelli ve olağan dışı durum temelli ağ saldırı belirleme yöntemleri çözüm olarak sunulmaktadır.

İmza temelli sistemler, incelenen veriler içerisinde tanımlanmış kalıpları ya da imzaları bulmaya çalışmaktadır. Bu amaçla bilinen saldırılara karşılık gelen kalıplar için bir veri tabanı oluşturulmaktadır. Diğer yandan, olağan dışı durum temelli sistemler, korunacak sistemin olağan davranışını öngörmeye çalışmakta ve belirli bir anda gözlemlediği davranış ile olağan davranış arasındaki sapmaya bakmaktadır. Bu yaklaşımda gözlemlenen sapma önceden tanımlanmış bir eşiği aştığında olağan dışı durum uyarısı üretilmektedir. Diğer bir yaklaşım ise sistemin olağan dışı davranışlarının modellenmesidir. Bu yaklaşımda, gözlemlenen davranış ile beklenen davranış arasındaki fark belirli bir sınırın altına düştüğünde uyarı oluşturulmaktadır.

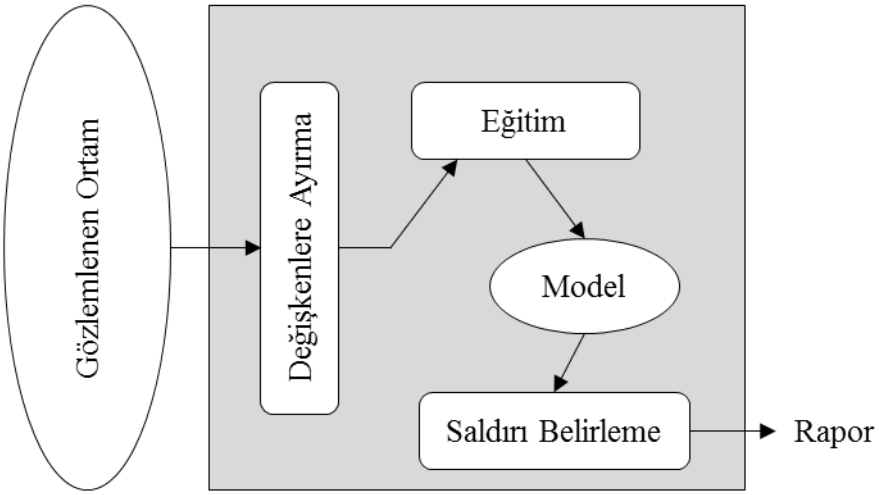
İmza temelli ve olağan dışı durum temelli sistemler kavramsal işleyiş açısından benzerlik göstermesine karşın saldırı ve olağan dışı durum kavramları bu iki yöntemi birbirinden ayırmaktadır. Saldırı bir bilgi sisteminin güvenliğini riske atan işlem dizisi olarak tanımlanırken; anormallik güvenlik açısından şüpheli bir olay olarak tanımlanmaktadır. Bu ayrımdan yola çıkılarak, imza temelli ve olağan dışı durum temelli yaklaşımların üstün ve eksik yönleri şu şekilde ifade edilebilmektedir.

İmza temelli sistemlerde, belirlenmiş ve bilinen saldırıların belirlenme oranı çok yüksek olmasına karşın yeni ve bilinmeyen saldırıların belirlenmesinde yetersiz kalmaktadır. Bu durum gözlemlenen saldırı, bilinen saldırılardan çok az farklı olsa bile yine yetersiz kalmaktadır. Diğer taraftan, olağan dışı durum temelli belirleme yönteminin en önemli üstünlüğü daha önce görülmemiş saldırı olaylarını belirlemedeki başarısıdır.

Aşağıda olağan dışı durum temelli belirlemede kullanılan yöntemler ve algoritmalar açıklanmıştır.

3.1 A-NIDS Teknikleri

Olağan dışı durum temelli saldırı belirleme sistemleri genel olarak Şekil 3.1'de gösterilen temel modüller veya aşamalardan oluşmaktadır. Değişkenlere ayırma aşamasında, hedef sistemin gözlemlenen verileri belirlenmiş formatta bir araya getirilmektedir. Eğitim aşamasında, sistemin olağan ya da olağan dışı davranışları otomatik ya da elle ayrılmakta ve buna karşılık gelen bir model oluşturulmaktadır. Belirleme aşamasında ise gözlemlenen trafik ile oluşturulan model karşılaştırılmakta ve sapma değeri gözlemlenmektedir [34].



Şekil 3.1 : Genel fonksiyonel mimari.

Hedef sisteme ilişkin davranış modelinin işlenme türüne göre olağan dışı durum temelli belirleme yöntemleri istatiksel temelli, bilgi temelli ve makine öğrenmesi temelli olarak üç ana sınıfta incelenmektedir [35]. İstatistik temelli yaklaşımlarda, sistemin davranışının rastgele olduğu varsayılmaktadır. Diğer yandan, bilgi temelli yaklaşımlarda protokol özellikleri, ağ trafik örnekleri gibi mevcut sistem verilerinden, beklenen davranışları yakalamaya çalışmaktadır. Makine öğrenmesi ise incelenen verilerin sınıflandırılmasını sağlayan bir modelin kurulmasına dayanmaktadır.

3.1.1 İstatiksel temelli yaklaşım

İstatiksel temelli yaklaşımlarda, ağ trafiği izlenmekte ve trafik yoğunluğu, her bir protokol için paket sayısı, bağlantı oranı, farklı IP adreslerinin sayısı gibi ölçülere dayanılarak, olasılıksal davranışını temsil eden bir profil oluşturulmaktadır.

Olağan dışı durum belirleme işlemi gerçekleştirilirken, zaman içerisinde gözlemlenen anlık profil ve önceden eğitilmiş istatiksel profil kullanılmaktadır. Bu kapsamda ağ üzerinde bir hareketlilik olduğunda mevcut profil belirlenmekte ve eğitilmiş model ile karşılaştırılarak, düzensizlik derecesini ifade eden bir olağan dışılık değeri üretilmektedir. Üretilen değerin belirli bir eşiği aşması durumunda ise olağan dışı durum oluştuğu ifade edilmektedir.

En eski istatistiksel yaklaşımlar tek değişkenli modellere karşılık gelmektedir. Bu yaklaşımda parametreler bağımsız Gauss rastgele değişkenleri [36] olarak modellenmekte, böylece her değişken için kabul edilebilir bir değer aralığı tanımlanmaktadır. Daha sonra ise iki veya daha fazla ölçüm arasındaki ilişkileri dikkate alan çok değişkenli modeller önerilmiştir [37]. Son olarak, gözlemlenen verilerin sıralarını ve varış zamanlarını dikkate alan zaman serili modeller üzerinde çalışılmıştır. Bu yaklaşımda, gözlemlenen bir trafik örneğinin belirli zamanda meydana gelme olasılığı çok düşük olduğunda trafik verisi olağan dışı durum olarak işaretlenmektedir.

İstatiksel yöntemlerin sağlamış olduğu üstünlük, sistemin olağan davranışı hakkında önceden bilgi gerektirmemesi bunun yerine sistemin beklenen davranışlarını yapmış olduğu gözlemlerden öğrenebilmesidir.

Eksikliği ise, saldırı sırasında oluşan ağ trafiğinin olağan kabul edilebilmesi ve modelin saldırgan tarafından eğitilmiş olmasıdır. Diğer bir eksikliği ise, yanlış pozitifler ve yanlış negatifler arasındaki dengenin kurulması için farklı parametrelerinin değerlerinin ayarlanması işlemi zorlayıcı bir çalışmadır. Ayrıca tüm davranışlar olasılıksal yöntemler kullanılarak modellenememektedir.

3.1.2 Bilgi temelli yaklaşım

Uzman sistem yaklaşımı en yaygın kullanılan bilgi temelli saldırı belirleme yöntemdir. Bu yaklaşım, deneyimli alan uzmanlarının ve karar vericilerin bilgi ve tercihlerini mantıksal kurallar şeklinde yansıtmayı amaçlamaktadır.

Uzman sistemler, denetim verilerini üç adımdan oluşan kurallara göre sınıflandırmayı amaçlamaktadır. İlk adımda eğitim verisi üzerindeki nitelikler ve sınıflar belirlenmektedir. İkinci adımda, sınıflandırma kuralları, parametreler veya yöntemler oluşturulmaktadır. Son adımda ise denetim verileri oluşturulan yapılara göre sınıflandırılmaktadır [36] [38].

Belirtim temelli yöntemler, diğer olağan dışı durum yöntemleri gibi sapma değerlerini inceleyerek saldırıları belirlemesine karşın diğer yöntemlere göre daha kısıtlayıcı özelliklere sahiptir. Bunun nedeni ise modelin, makine öğrenmesi teknikleri yerine, kuralların kullanılarak oluşturulması ve bu sürecin bir uzman tarafından yürütülmesidir.

Belirtimlerin yeterince açık ve kapsamlı tanımlandığı durumlarda, model olağan dışı durum davranış kalıplarını belirleyebilmektedir. Ayrıca zararsız faaliyetlerin rapor edilmemesi nedeniyle yüksek oranda üretilen yanlış uyarılar bu yaklaşım ile azaltılmaktadır [39].

Olağan dışı durum belirlemeye yönelik mevcut yaklaşımların en önemli üstünlükleri sağlamlık ve esneklik olmalarıdır. Bu karşın ayrıntılı bilginin işlenmesi genellikle zor olduğu ve zaman aldığı için yaklaşımın kullanımı oluşturmaktadır. Bu sorun olağan kavramının sadece eğitim verilerinin incelenmesiyle elde edilen diğer olağan dışı durum yöntemlerinde de yaygın olarak görülmektedir.

3.1.3 Makine öğrenmesi yaklaşımı

Öğrenme, örnek bir veri kümesinden bilgi edindikten sonra bilimsel bir model oluşturma süreci olarak tanımlanmaktadır. Makine öğrenmesi de bilgisayar temelli bir kaynağın kullanılarak öğrenme algoritmalarının gerçekleştirilmesidir. Böylece bilgisayarların açık bir şekilde programlanmadan hareket etmesi sağlanmaktadır.

Makine öğrenmesinin görüntü tanıma, akıllı karar sistemlerinin geliştirilmesi, kendi kendini süren araçların üretilmesi, el yazısı ve konuşma tanıma, etkili web araması gibi birçok alanda kullanıldığı görülmektedir.

Makine öğrenmesi genel olarak aşağıdaki gibi üç kategoriye ayrılmaktadır.

- Denetimli öğrenme
- Denetimsiz öğrenme
- Yarı denetimli öğrenme

Denetimli öğrenme algoritmaları kullanılarak bir model oluşturulmak istendiğinde kullanılacak veri kümesinin etiketli olması gerekmektedir. Bir diğer ifade ile giriş değerleri için sonuç değerlerinin bilinmesi gerekmektedir. Verilerin etiketlenmesi işlemi genellikle makine öğrenmesi hakkında bilgiye sahip veri analisti ya da veri bilimcisi tarafından yapılmaktadır.

Denetimli öğrenme kendi içerisinde sınıflandırma ve regresyon olarak ikiye ayrılmaktadır. Sınıflandırma algoritmalarında çıktı değerleri “beyaz”, “mavi”, “yeşil” ya da “var”, “yok” gibi sınıflandırılmaktadır. Bu algoritmalarda her bir girdi için belirlenmiş sınıflardan en uygunu seçilerek sonuç ataması yapılmaktadır. Regresyon algoritmalarında ise gerçek sayısal bir değer üretilmektedir. Örneğin bir insanın ağırlığı ya da bir evin satış fiyatı belirlenmek istendiğinde önceki değerlere bakılarak yeni sayısal bir değer üretilmektedir.

Denetimsiz öğrenme algoritmalarında giriş verileri için bir çıkış değeri (etiketleme) bulunmamaktadır. Bu algoritmalar benzer özellikte olan verileri aynı grupta toplayarak yeni gelen verinin hangi gruba ait olduğunu belirlemeye çalışmaktadır.

Yarı denetimli öğrenme algoritmalarında, etiketlenmiş ve etiketlenmemiş verilerin birleştirilmesiyle oluşan bir veri kümesi üzerinde eğitme işlemi yapılmaktadır. Denetimli öğrenme için büyük miktarlarda verinin etiketlenmesi genellikle çok zaman alıcı ve pahalı bir süreçtir. Ayrıca çok fazla etiketlemenin yapılması oluşturulan modelin karar verirken ezberlemesine ve önyargıda bulunmasına neden olabilmektedir. Diğer taraftan model oluşturulurken modele etiketlenmemiş verilerin eklenmesi son modelin doğruluğunu arttırırken model oluşturma zamanını ve maliyeti azaltmaktadır.

Çizelge 3.1'de makine öğrenmesi kapsamında kullanılan algoritmalar gösterilmektedir.

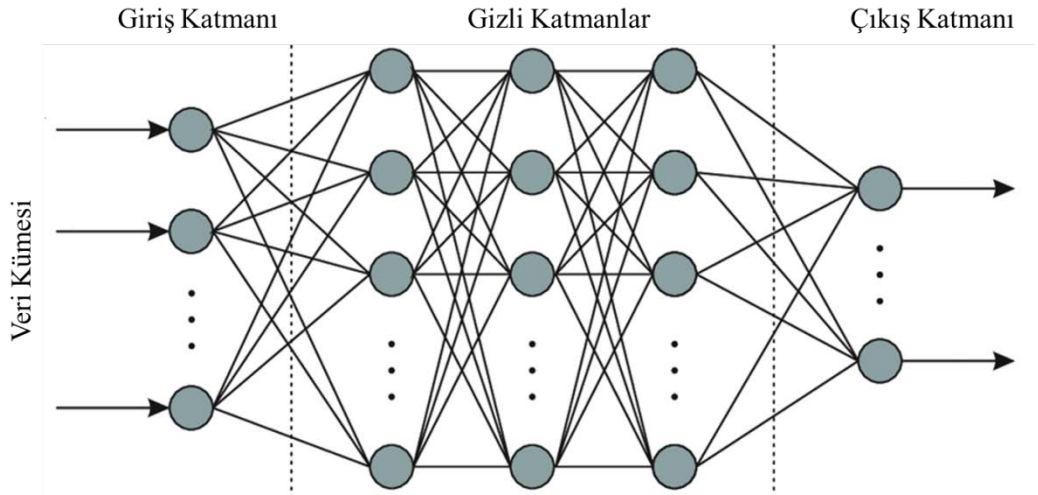
Çizelge 3.1 : Makine öğrenmesi algoritmaları.

Denetimli Öğrenme	Denetimsiz Öğrenme	Yarı Denetimli Öğrenme
Association Rule Classification	k-ortalama	Süreklilik varsayımı
Yapay Sinir Ağları	Beklenti maksimizasyonu	Kümeleme varsayımı
Support Vector Machines	k-en yakın komşu	Çoğaltma varsayımı
Karar Ağaçları	SOM ANN	Üretici modeller
Bayes Ağları	PCA	Düşük yoğunluk ayrımı
Hidden Markov Model	Alt alan kümeleme	Çizge temelli yöntemler
Kalman Filtresi		Sezgisel yaklaşımlar
Bootstrap, Bagging, and AdaBoost		
Random Forest		

3.2 Derin Öğrenme

Derin öğrenme, makine öğrenmesinin alt bir kümesi olarak geliştirilmiştir. Derin öğrenmede insan beyninin yapısı ve işlevselliği esinlenerek oluşturulmuş yapay sinir ağları kullanılmaktadır. Farkları ise biyolojik beyinde herhangi bir nöron belirli bir fiziksel mesafe içinde başka bir nörona bağlanabilirken yapay sinir ağları ayrı katmanlara, bağlantılara ve veri yayılımına sahiptir.

Yapay sinir ağlarında eğitilmek istenen veriler Şekil 3.2 ’de görüldüğü gibi ilk olarak sinir ağının ilk katmanına girmektedir. İlk katmanda yer alan bireysel nöronlar veriyi ikinci katmana geçirmektedir. Bu katmanda nöronlar işini tamamladığında veriyi diğer katmana geçirmekte ve son katmana ulaşarak nihai sonuç üretilinceye kadar bu işlem devam etmektedir. Bu işlemler sırasında her nöron giriş verisi için gerçekleştirilmek istenen görevin doğruluğuna ya da yanlışlığına göre bir ağırlık değeri vermektedir. Nihai sonuç ise bu ağırlıkların toplamına göre belirlenmektedir [40].



Şekil 3.2 : Yapay sinir ağları.

Son zamanlara kadar sinir ağlarının kullanımı yapay zeka araştırma topluluğu tarafından reddedilmekteydi. Çünkü en basit sinir ağlarının eğitilmesi bile yoğun hesaplama gerektirmesi nedeniyle pratik bir yaklaşım olarak görülmemekteydi. Bu sonunun aşılması için Toronto Üniversitesinde Geoffrey Hinton ve arkadaşları [41] tarafından süper bilgisayarlar için paralel algoritmaların geliştirilmesi kapsamında çalışmalar yürütülmüştür. Sonraları grafik işlem ünitelerinin (GPU) üretimiyle birlikte yoğun hesaplamaları kolaylıkla yapabilen yeterince büyük ve hızlı bilgisayarlar üretilmiştir. Büyük sinir ağlarını eğitecek kadar verinin toplanması ve işlem gücü yüksek bilgisayarların geliştirilmesi derin öğrenmenin temeli oluşturmuştur.

3.3 Ağ Davranış Çözümlemesi

Ağ Davranış Çözümlemesi, ağ güvenliğinin arttırılması amacıyla ağ trafiğinin izlenmesi ve olağan dışı durumların belirlenmesi yöntemidir. Bu yaklaşım genellikle iç ağlara odaklanmaktadır.

Geleneksel saldırı belirleme sistemleri paket denetimi, imza temelli saldırı belirleme ya da gerçek zamanlı engelleme gibi yaklaşımları kullanmaktadır. Ağ Davranış Çözümlemesi yaklaşımı ise çevrimdışı incelemeyi desteklemek için birçok veri noktasından bant genişliği ve protokol kullanımları gibi bilgileri toplayarak ağ içinde oluşan durumları izlemektedir.

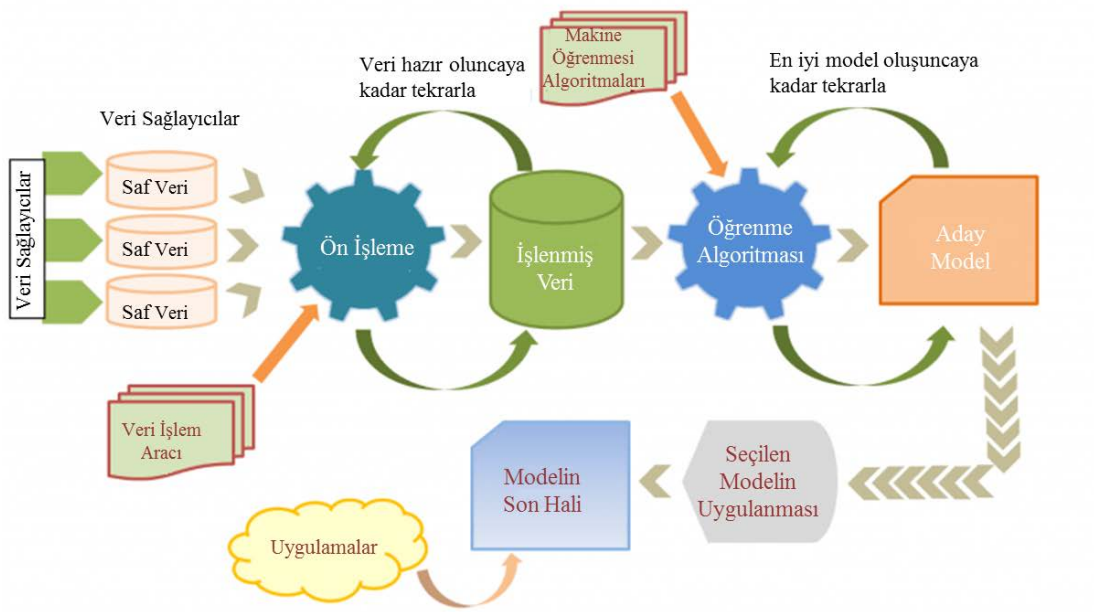
Normal trafik bilgisi toplanarak bir referans noktası oluşturulduktan sonra ağ davranış çözümlemesi uygulamaları pasif olarak ağda meydana gelen durumları izlemekte ve saldırı olarak değerlendirilebilecek bilinmeyen, yeni oluşan ya da olağan dışı durumları işaretlemektedir. Bu özelliği sayesinde kişilerin olağan dışı davranışlarının, yeni kötü amaçlı yazılımların ve sıfır gün istismarlarının belirlenmesinde diğer yaklaşımlara göre üstünlüğü bulunmaktadır.

Tez kapsamında kullanılarak kurum içi ağlarda oluşan olağan dışı durumların belirlenmesi amacıyla Ağ Davranışlarında Olağan Dışı Durumların Belirlenmesi (Network Behaviour Anomaly Detection - NBAD) yöntemi kullanılmaktadır.

4. GELİŞTİRİLEN YÖNTEM

Bilgisayarların ve sahip oldukları işlem yeteneklerinin gelişmesiyle birlikte kısa süre içerisinde karmaşık hesaplamalar rahatlıkla yapılmaya başlanmıştır. Bu da farklı araştırma ve kullanım alanlarının oluşmasına neden olmuştur. Bu alanlardan birisi de modellere bakarak olası bir sonucu öngörmeye çalışan makine öğrenmesi yöntemleridir.

Makine öğrenmesi yöntemlerinin genel kullanımı Şekil 4.1'de gösterildiği gibi verilerin toplanması, verilerin düzenlenmesi ve uygun özniteliklerin seçimi, modelin oluşturulması (eğitim) ve değerlendirme süreçlerinden oluşmaktadır.



Şekil 4.1 : Makine öğrenmesi süreçleri.

Tez kapsamında ağ üzerindeki davranışlar incelendiği için ağ modelinin oluşturulması, yeni oluşan durumun oluşturulmuş modele uygunluğunun değerlendirilmesi ve ağa ya da ağ üzerindeki bilgisayarlara saldırı olup olmadığı sonucunun üretilmesi bakış açısıyla hareket edilmiştir.

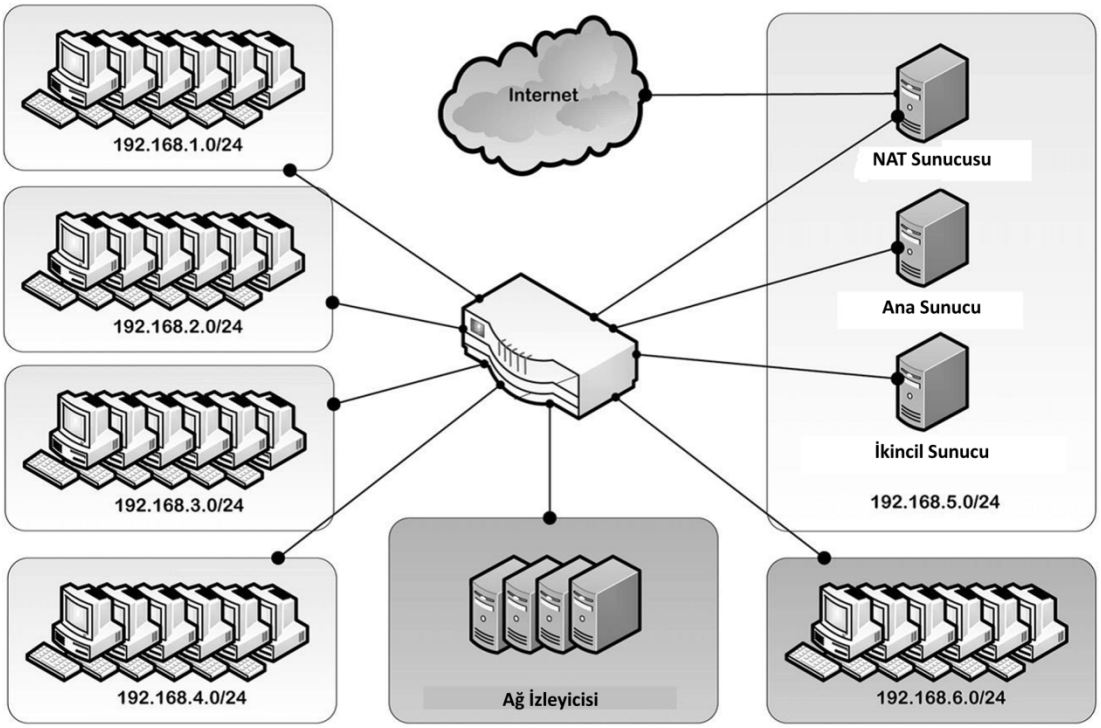
4.1 Veri Kümesi

Olağan dışı durum temelli saldırı belirleme yaklaşımlarında yeterli ve uygun veri kümesinin olmamasından kaynaklı değerlendirme, karşılaştırma ve geliştirme işlemlerinde zorluklar yaşanmaktadır. Bu veri kümelerinin çoğu içsel olduğu için gizlilik nedeniyle paylaşılamamaktadır. Anonimleştirilen veri kümeleri ise güncel olmamakla birlikte belirli istatiksel özelliklerden de yoksun olabilmektedir.

Ağ davranışlarının ve kalıpların değişmesi, ağa yapılan saldırıların gelişmesi nedeniyle statik ve tek kullanımlık veri kümeleri yerine değiştirilebilir, genişletilebilir ve güncellenebilir dinamik olarak oluşturulmuş veri kümelerine gerek duyulmaktadır. Bu gereksinimin giderilmesine yönelik, ISCX (Information Security Center of Excellence) tarafından gerekli veri kümelerinin üretilmesi için sistematik bir yaklaşım sunulmuş [42] ve Saldırı Belirleme ve Değerlendirme UNB ISCX IDS 2012 [43] veri kümesi üretilmiştir.

UNB ISCX IDS 2012 veri kümesi, olağan dışı durum temelli saldırı belirleme sistemlerinin geliştirilmesine yardımcı olmak için 2010 yılında üretilmeye başlanmış ve 2016 yılına kadar geliştirilmeye devam edilmiştir. Veri kümesi içerisinde olağan olmayan davranışların oluşturulması amacıyla çok aşamalı saldırı senaryoları kullanılmış ve ağ trafik verileri olağan ve olağan olmayan olarak etiketlenmiştir.

Veri kümesinin oluşturulması aşamasında Şekil 4.2’de yer alan sınama ortamı ağ mimarisi kullanılmıştır. Sınama ağ mimarisi içerisinde 21 tane birbirine bağlı Windows iş istasyonu bulunmaktadır. Bu iş istasyonlarından 17 tanesi Windows XP S1, 2 tanesi Windows XP S2, 1 tanesi Windows XP S3 ve 1 tanesi Windows 7 işletim sistemlerine sahiptirler. Windows işletim sistemlerine ilişkin bilinen çeşitli güvenlik açıkları bulunmakta ve bulunan her açıklık güncel olarak CVE (Common Vulnerabilities and Exposures) 'nin [33] sitesinde duyurulmaktadır. Bilinen bu açıklıklardan yararlanmak amacıyla sınama ortamı oluşturulurken Windows işletim sistemlerinin kullanıldığı belirtilmektedir.



Şekil 4.2 : Sınama ortamı ağ mimarisi.

Oluşturulan bu ağ mimarisi ile yerel ağ bağlantısı (LAN) içerisindeki trafik ve yerel ağ bağlantıları arasındaki trafik izlenebilmektedir. Bu kapsamda sınama ortamı üzerinde yedi gün boyunca Wireshark [44] ağ izleme aracı ile ağdaki paket akışı izlenerek .pcap uzantılı dosyalar içerisine kayıt edilmiştir. İzlenen paket akışlarının toplam boyutu ve paket sayısı Çizelge 4.1 ‘de yer almaktadır.

Çizelge 4.1 : Veri kümesi günlük veri boyutları.

Veri Kümesi	Boyut (GB)	Paket Sayısı
1.Gün	16.1	21478494
2.Gün	4.22	5973980
3.Gün	3.95	11438288
4.Gün	6.85	9623281
5.Gün	23.4	35001060
6.Gün	17.6	24541442
7.Gün	12.3	17330491

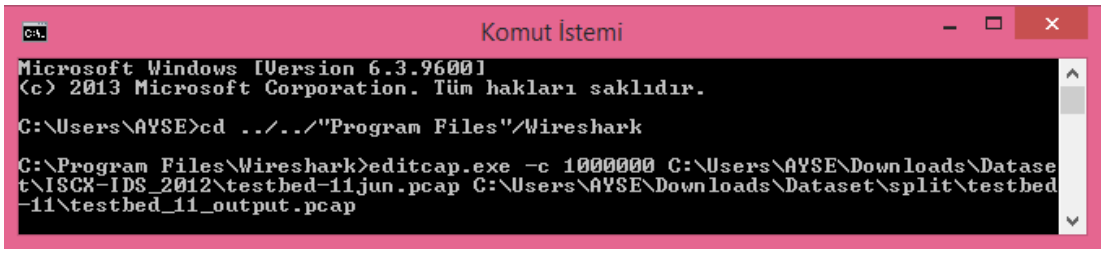
Veri kümesinin eğitilebilmesi için içerisinde yer alan bilgilerin anlamlı hale getirilmesi gerekmektedir. Bu kapsamda veriler ve verilerin birbirleriyle olan ilişkileri incelenerek yeni verilerin üretilmesi, var olan verilerin düzeltilmesi ya da silinmesi işlemleri verilerin incelenmesi ve öznitelik çıkarımı başlığı altında anlatılmıştır.

4.2 Verilerin İncelenmesi ve Özniteliklerin Çıkarılması

Özniteliklerin çıkarılması, özgün veri kümesi içerisinde yer alan bilgilerin işletilebilir ve yönetilebilir hale getirilmesi için yapılan boyut küçültme işlemi olarak tanımlanmaktadır. Bu yaklaşım modelin doğruluğuna katkıda bulunmayan ya da doğruluğunu azaltabilen verilerden gereksiz ve ilgisiz olanlarının bulunması ve kaldırılması için kullanılmaktadır [45].

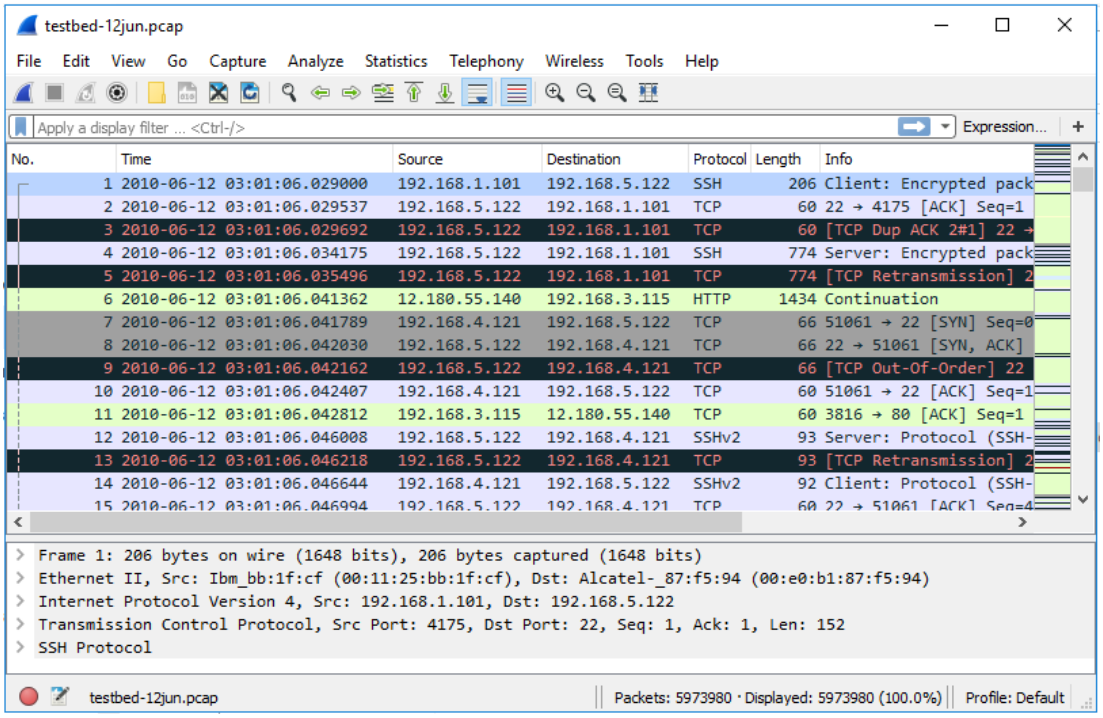
Tez kapsamında kullanılan UNB ISCX IDS 2012 özgün veri kümesi Wireshark ağ izleme aracı kullanılarak elde edilen verilerden oluşmaktadır. Wireshark ağ izleme aracı üzerinden toplanan veriler, ağ üzerindeki bütün bilgileri içermeleri nedeniyle işlenmemiş veri olarak tanımlanmaktadır. Bu veriler doğrudan makine öğrenmesi algoritmalarında kullanılamamaktadır. Ayrıca rastgele her bilginin kullanımı model eğitme işleminin daha uzun sürmesine neden olmakta ve modeli karmaşıklaştırmaktadır. Bundan kaynaklı olarak yanlış sonuçların üretimi artmaktadır. Bu nedenle Wireshark temelli .pcap dosyalarında yer alan ağ paketleri incelenerek uygun parametreler çıkarılmıştır. Bu işlem sırasında aşağıda bahsedilen adımlar sırasıyla izlenmiştir.

İlk aşamada, kullanılacak verilerin incelenebilmesi ve üzerinde çalışma yapılabilmesi amacıyla Wireshark aracının bir programı olan editcap.exe kullanılarak .pcap dosyaları boyutu daha küçük olan dosyalara bölünmüştür (Şekil 4.3).



Şekil 4.3 : Editcap.exe ekran görüntüsü.

İkinci aşamada, Wireshark aracına bölünmüş veri kümeleri yüklenerek ağ akışına ilişkin paket yapıları incelenmiştir (Şekil 4.4).



Şekil 4.4 : Wireshark ağ izleme aracı.

Çizelge 4.2 ‘de veri kümesinde yer alan protokoller ve protokollerin ilişkin olduğu OSI katmanı gösterilmektedir. ARP paketi veri bağlantı katmanında IP ve MAC eşleştirmesi yapan bir protokol olduğu için paket içerisinde IP bilgisi ve port bilgisi bulunmamaktadır. Ayrıca ICMPv6 paketinde de port bilgisi yer almamaktadır.

Çizelge 4.2 : Veri kümesinde yer alan protokoller.

OSI Katmanları	Kullanılan Protokoller
Fiziksel Katman	-
Veri Bağlantı Katmanı	ARP
Ağ Katmanı	IP, ICMP, ICMPv6, DHCPv6
Taşıma Katmanı	TCP, UDP
Uygulama Katmanı	HTTPS, FTP, SSH, SMTP, POP, IMAP, DNS, NBNS, MDNS, LLMNR, NBSS, SMB, LANMAN, Browser

Üçüncü aşamada, Wireshark aracının terminal yönelimli sürümü olan TShark kullanılarak Çizelge A.1 ’de yer alan veriler .pcap uzantılı dosyalardan ayrıştırılarak .csv uzantılı dosyalara yazılmıştır (Şekil 4.5).

```
Komut İstemi
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\AYSE>cd ../../"Program Files"/Wireshark

C:\Program Files\Wireshark>tshark -r C:\Users\AYSE\Downloads\Dataset\ISCX-IDS_20
12\testbed-12jun.pcap -T fields -e frame.number -e frame.time_epoch -e frame.len
 -e _ws.col.Protocol -e arp -e ip.src -e ip.dst -e ip.version -e ip.proto -e ip.
flags.mf -e ip.ttl -e icmp -e icmpv6 -e dhcpv6 -e igmp -e udp.stream -e udp.srcp
ort -e udp.dstport -e tcp.stream -e tcp.srcport -e tcp.dstport -e tcp.flags.ack
-e tcp.flags.push -e tcp.flags.reset -e tcp.flags.syn -e tcp.flags.fin -e tcp.an
alysis.duplicate_ack -e tcp.analysis.retransmission -e tcp.analysis.fast_retrans
mission -e tcp.analysis.spurious_retransmission -e tcp.analysis.out_of_order -e
tcp.analysis.zero_window -e tcp.analysis.keep_alive -e tcp.analysis.ack_rtt -e t
cp.analysis.reused_ports -e http -e http.request -e http.response -e http.respon
se.code -e http.leading_crlf -e pop -e pop.response.indicator -e smtp -e smtp.re
sponse.code -e imap -e imap.line -e dns -e dns.qry.type -e dns.flags.response -e
 dns.flags.rcode -e dns.retransmission -e dns.retransmit_request -e dns.retransm
it_response -e nbns -e nbns.flags.broadcast -e nbns.flags.response -e nbns.flags
.rcode -e mdns -e llmnr -e ssh -e ftp -e ftp.request -e ftp.request.command -e f
tp.response -e ftp.response.code -e ftp.response.code.invalid -e nbss -e nbss.ty
pe -e smb -e lanman -e browser -e browser.server_type.workstation -e browser.ser
ver_type.server -e browser.server_type.sql -e browser.server_type.browser.master
 -e browser.server_type.browser.potential -E header=y -E separator=, > C:\Users\
AYSE\Downloads\Dataset\csv\test12.csv_
```

Şekil 4.5 : Kullanılacak verilerin TShark ile .csv formatına dönüştürülmesi.

Dördüncü aşamada, veriler anlamlı hale getirilmiştir. TShark ile elde edilen dosyada birden fazla verinin tekrarı bulunmaktadır. Örneğin TCP kaynak port numarası ve UDP kaynak port numarası iki ayrı alana sahiptir. Bir paket içerisinde aynı anda hem UDP hem TCP bilgisi olamayacağı için bu iki bilgi birleştirilerek kaynak port numarası olarak tek bir özniteliğin altında birleştirilmiştir. Ayrıca protokol ismi gibi metin verileri one-hot encoding yöntemi [46] ile mantıksal hale getirilmiştir.

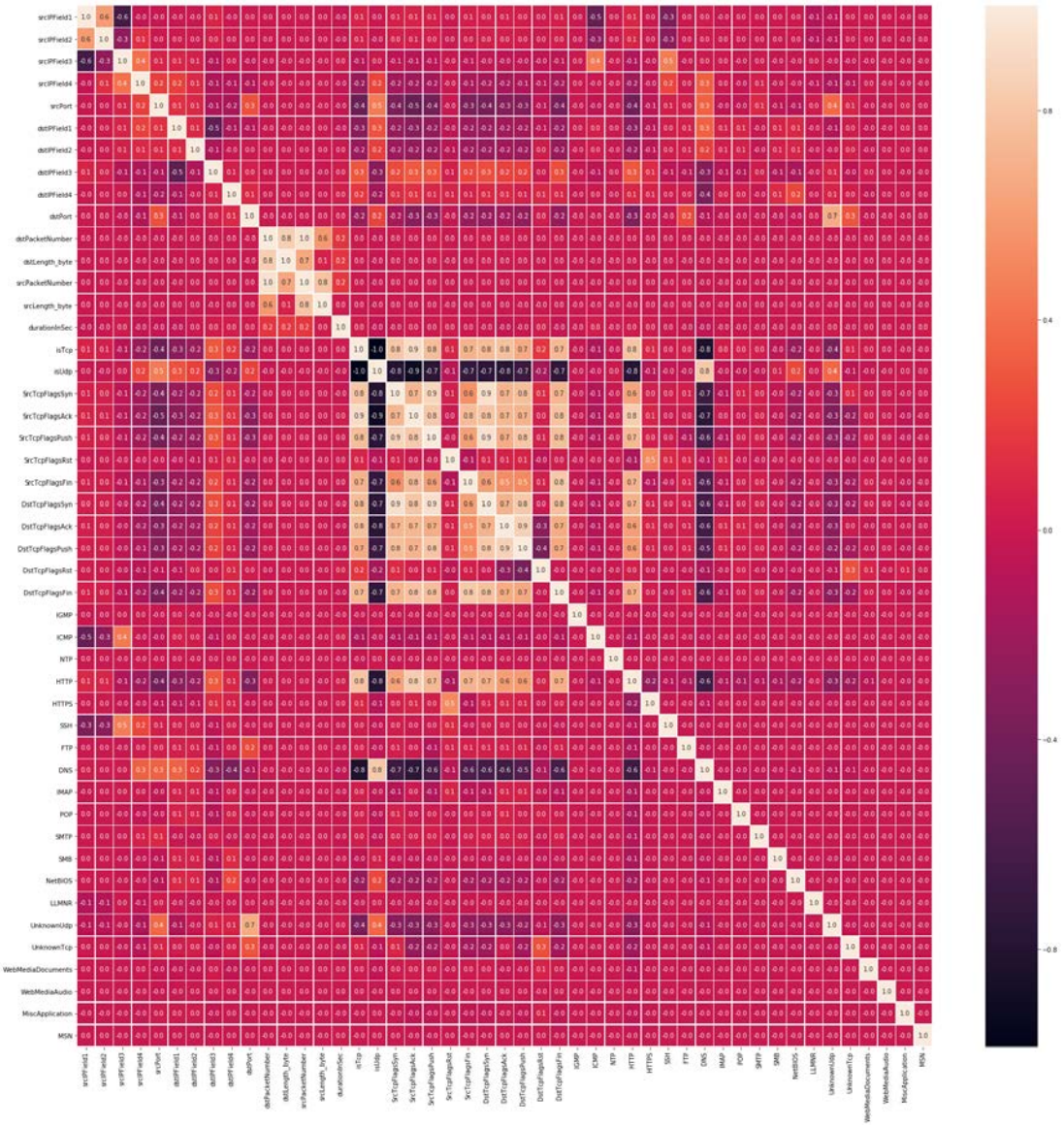
Son aşamada ise, aynı kaynak adrese, hedef adrese, kaynak port numarasına ve hedef port numarasına sahip paketler bir araya getirilerek NetFlow [47] standartlarında veri akışı oluşturulmuştur. Oluşturulan veri akışı ile ISCX tarafından paylaşılan XML dosyasında yer alan saldırı bilgileri birleştirilerek ve Çizelge A.2 :'de yer alan bilgiler kullanılarak eğitilmek üzere bir eğitim veri seti oluşturulmuştur. Veri kümesindeki her gün için ayrı ayrı bu işlem gerçekleştirildikten sonra veriler birleştirilerek tek bir veri kümesi haline getirilmiştir. Oluşturulan akış bilgisi Çizelge 4.3'de gösterilmektedir.

Çizelge 4.3 : Akış verileri.

Gün	Akış Sayısı	TCP Akış Sayısı	UDP Akış Sayısı	ICMP Akış Sayısı	Olağan	Olağan Olmayan
1.Gün	378667	297398	78786	2478	378667	0
2.Gün	133193	95117	37966	95	131107	2086
3.Gün	275528	221026	54076	374	255170	20358
4.Gün	171380	122298	48453	623	167609	3771
5.Gün	571701	441563	124023	6073	534323	37378
6.Gün	522265	434674	87070	513	522265	0
7.Gün	397595	329378	67658	547	392392	5203

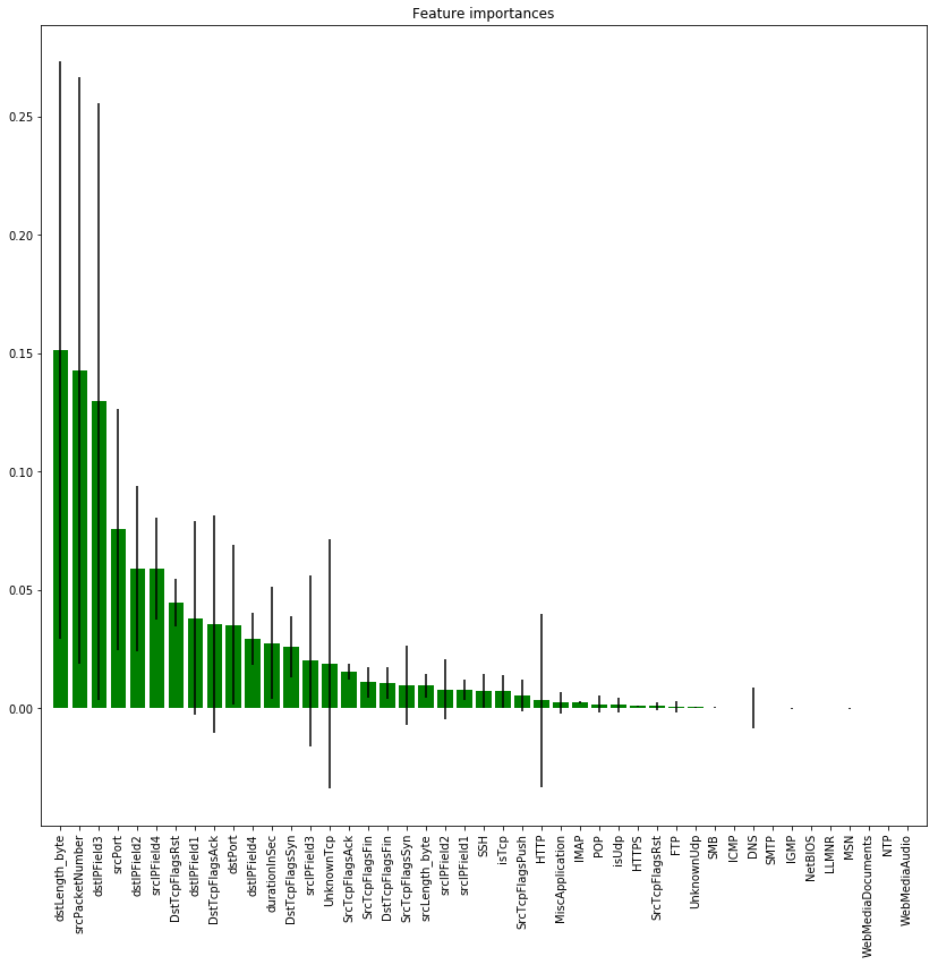
Öğrenme adımında kullanılabilecek anlamlı bir veri kümesi oluşturulduktan sonra bu veri kümesi içinde yer alan özniteliklerin modele etkisini gözlemlemek amacıyla bağdaşma, tek değişkenli öznitelik seçimi, yinelemeli öznitelik eleme (RFE) ve çapraz doğrulama ile yinelemeli öznitelik eleme (RFECV) yöntemleri kullanılabilmektedir. Bu yöntemler aracılığıyla veri kümesinde yer alan önemli öznitelikler seçilerek diğer öznitelikler veri kümesinden çıkarılabilmektedir.

Bağdaşma yönteminde bütün özniteliklerin birbiriyle olan ilişkisini göstermek için grafik haritası kullanılmaktadır. Şekil 4.6‘da veri kümesine ilişkin özniteliklerin grafik haritası gösterilmektedir. Bu grafiğe göre dstPacketNumber ve srcPacketNumber öznitelikleri arasında ve dstTcpFlagsAck ve dstTcpFlagsPush öznitelikleri arasında bağdaşma olduğu gözlemlenmektedir. Bu nedenle srcPacketNumber ve dstTcpFlagsAck öznitelikleri seçilerek bağdaşma içeren diğer öznitelikler veri kümesinden çıkarılmıştır.



Şekil 4.6 : Bağdaşma grafik haritası.

Özniteliklerin önemlilik oranı belirlenirken veri kümesi içinde bağdaşma içeren özniteliklerin olmaması gerekmektedir. Şekil 4.7'de önemi yüksek özniteliklerin oran grafiği gösterilmektedir. Bu grafiğe göre Çizelge A.3'te listelenen özniteliklerin model oluşturma aşamasında daha önemli olduğu görülmektedir.



Şekil 4.7 : Önemi yüksek özniteliklerin oran grafiği.

4.3 Model Oluşturma

Model oluşturma süreci makine öğrenmesi algoritmasının seçilmesi, seçilen algoritma ile aday bir modelin oluşturulması, aday modelin sınanması ve yeterince iyi sonuç verinceye kadar bu işlemlerin tekrarlanması aşamalarını içermektedir.

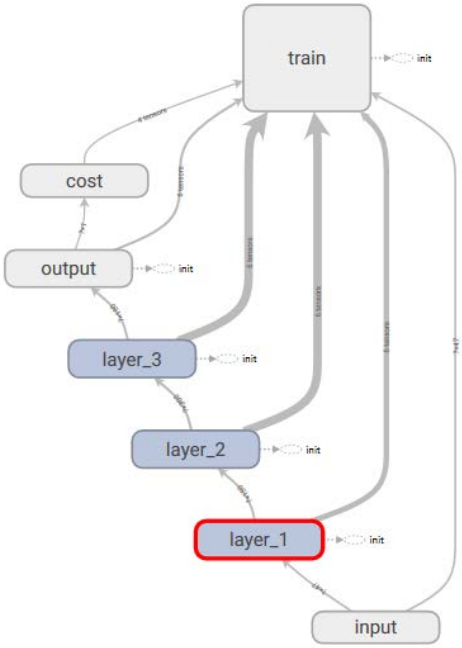
Ağ davranış modelleri oluşturulurken farklı yöntemlerden faydalanılabilmektir. Yöntemlerden birisi olağan davranışları içeren modelin oluşturulması ve yeni davranışın oluşturulmuş davranış modeline uyup uymadığına bakılarak olağan ya da olağan olmayan durum kararının verilmesidir. Diğer bir yaklaşım sadece olağan olmayan davranışların belirlenerek saldırıların olağan olmayan davranışlar içinde aranmasıdır. Bu yaklaşım başarım açısından kazanç sağlamasına karşın bütün olağan olmayan durumların belirlenmesi olanaksız olacağı için yetersiz kalmaktadır. Bir diğer yaklaşım ise hem olağan hem olağan olmayan durumların kullanılarak bir sınıflandırma modelinin oluşturulmasıdır.

Tez kapsamında, ağda meydana gelen olağan dışı durumların belirlenebilmesi için olağan ve olağan olmayan davranışları içeren veri kümesi kullanılarak sınıflandırma modeli oluşturulmuştur. Sınıflandırma modeli oluşturulurken "Ağ Davranışı Çözümleme" yaklaşımı kullanılmıştır. A-NIDS yaklaşımları ağda gördüğü her paketi incelerken "Ağ Davranış Çözümlemesi" ağ üzerindeki akışları incelemektedir. Verilerin düzenlenmesi aşamasında ağ paketlerinden aynı amaca hizmet edenler birleştirilerek veri akışını içeren veri kümesi oluşturulmuştur. Bu aşamada ise oluşturulmuş veri kümesi ve öğrenme algoritmaları kullanılarak eğitme işlemi yapılmaktadır.

Saldırıların belirlenmesi kapsamında model oluşturulurken derin öğrenme algoritmalarını içeren TensorFlow kütüphanesi kullanılmıştır. Önceleri SVM, k-ortalama, karar ağaçları gibi sığ makine öğrenmesi algoritmaları yaygın olarak kullanılırken 2015 yılında TensorFlow [48] kütüphanesinin kullanımıyla birlikte makine öğrenmesinin bir alt kümesi olan derin öğrenmeye geçilmiştir.

TensorFlow, veri akışı grafiklerini kullanarak sayısal hesaplamalar için geliştirilmiş açık kaynaklı bir yazılım kütüphanesidir. Google Brain ekibi tarafından başlarda sadece makine öğrenmesi ve derin sinir ağları araştırmaları için geliştirilmesine karşın şu an birçok alanda uygulanabilecek kadar genel bir tasarıma sahiptir. Görüntü tanıma, doğal dil işleme gibi alanlarda yaygın olarak kullanılan kütüphane saldırıların belirlenmesine yönelik çalışmalarda da kullanılmaktadır. 2011 yılında geliştirilmeye başlanan ve 2015 yılında genel kullanıma açılan kütüphane önceleri tek bir makine üzerinde çalışabilirken, 2017 yılında yayınlanan 1.0 sürümü ile çoklu merkezi işlem birimlerinde (CPU) ve grafik işlemci ünitelerinde (GPU) ayrıca mobil (Android ve iOS) ve gömülü platformlarda çalışabilmektedir.

Çalışma sırasında TensorFlow kütüphanesinde yer alan ANN (Artificial Neural Network - Yapay Sinir Ağları) [40] algoritması kullanılmıştır. ANN, veriden öğrenen bir bilgisayar programı oluşturma yöntemidir. Bu yöntemde ilk olarak Şekil 4.8'de gösterildiği gibi birbirlerine mesaj gönderebilen yazılım nöronları oluşturulmakta ve birbirine bağlanmaktadır. Sonraki aşamada ise sorunun çözülmesi amacıyla başarıya giden bağlantıların güçlendirilmesi ve başarısızlığa neden olan bağlantıların azaltılması işlemi tekrar tekrar yapılmaktadır.



Şekil 4.8 : ANN grafik gösterimi.

Eğitme işlemine başlamadan önce eğitim ve sınama verilerinin ayrılması gerekmektedir. Kullandığımız veri kümesi yedi ayrı günden toplanan verileri içerdiği için ilk altı güne ilişkin veriler eğitim veri kümesi, yedinci güne ait veriler ise sınama veri kümesi olarak kullanılmıştır.

Model oluşturma aşamasında modele ilişkin değişkenlerin tanımlanması gerekmektedir. Tanımlanan bu değişkenler modelin öngörü başarı oranını etkilemektedir. ANN algoritması kullanılarak hazırlanan modellerde katman sayısının ve her katmanda yer alacak nöron sayısının belirtilmesi gerekmektedir. Yapılan çalışmalar sırasında Çizelge A.2'de yer alan öznitelikler kullanılarak giriş katmanı, çıkış katmanı ve 3 gizli katmandan oluşan toplamda 5 katmanlı ve 100 – 400 – 200 nöron değerleri ile oluşturulan modelin daha iyi sonuç verdiği gözlemlenmiştir. Sonuçlara ilişkin karşılaştırmalar değerlendirme aşamasında anlatılmaktadır.

TensorFlow kütüphanesi kullanılarak oluşturulan modellerin eğitimi grafik işlemci üniteleri kullanılarak daha hızlı yapılabilmektedir. TensorFlow şu an için sadece NVIDIA [49] tarafından üretilmiş ve işlemci kapasitesi 3,5 ve üstünde olan grafik işlem üniteleri üzerinde çalışabilmektedir. Ayrıca Google Colab [50] bulut servisi derin öğrenme üzerinde çalışan ve çalışma ortamlarında uygun grafik işlemcisi bulunmayan araştırmacılar için GPU desteği sağlamaktadır.

4.4 Değerlendirme

Değerlendirme aşaması üretilen modelin başarı oranının incelenmesi ve başarısız olarak nitelendirildiği durumlarda farklı algoritmalar ya da aynı algoritmanın farklı değişkenleri ile modelin yeniden eğitilerek sonuçların karşılaştırılması aşamasıdır.

Çalışma kapsamında Çizelge A.2 ’de gösterilen öznitelikleri içeren veri kümesi ve öznitelik seçim yöntemiyle azaltılmış Çizelge A.3 ’te gösterilen öznitelikleri içeren veri kümesi kullanılarak eğitim modelleri oluşturulmuştur. Model oluşturma sürecinde kullanılan yapay sinir ağları algoritmasına ilişkin gizli katmanda bulunan nöron değişkeninin değerleri değiştirildiğinde elde edilen doğruluk sonuçları farklılık göstermektedir.

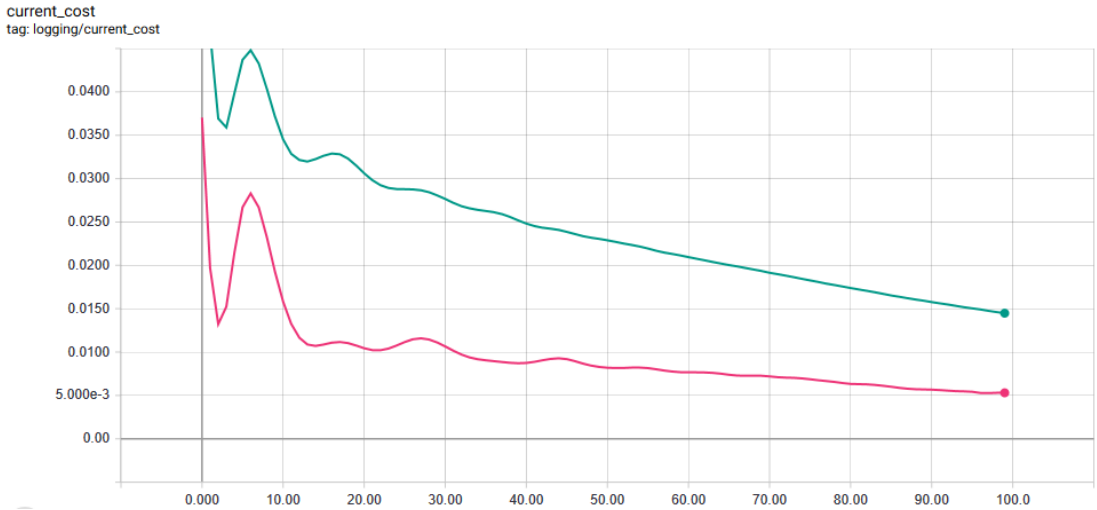
Maliyet fonksiyonu, kullanılan değişkenlerin veri kümesine göre ne kadar yanlış olduğunu ifade etmekte ve maliyet değerinin düşmesi doğruluk oranının arttığını göstermektedir. Bu bakış açısı göz önünde bulundurularak gizli katmanda bulunan nöron değerlerinin değiştirilmesiyle oluşturulmuş modellerin maliyet grafikleri çıkartılmıştır.

Bu kapsamda nöron sayısının değiştirilmesiyle elde edilen sonuçlar aşağıda yer almaktadır.

4.4.1 Çizelge A.2 ’de yer alan özniteliklerin kullanımıyla elde edilen sonuçlar

Şekil A.1’de, Çizelge A.2’de gösterilen 47 adet özniteliği içeren veri kümesi kullanılarak ve nöron sayısı değiştirilerek oluşturulan modeller için üretilmiş maliyet grafikleri yer almaktadır. Bu maliyet grafiklerinden 50 – 100 – 50 ve 150 – 300 – 150 nöron değerleri kullanılarak üretilmiş maliyet değer tablosu ve grafikleri aşağıda açıklanmıştır.

Şekil 4.9 ve Çizelge 4.4’de gizli katman sayısı 3 ve nöron sayısı 50 – 100 – 50 olan eğitilmiş modelinin sonuçları gösterilmektedir. Şekil üzerinde yeşil renk eğitim maliyetlerine, koyu pembe renk ise sınama maliyetlerine ilişkin grafiği göstermektedir. Grafikte X ekseni durum ilerlemesini Y ekseni ise maliyet değerlerini ifade etmektedir.



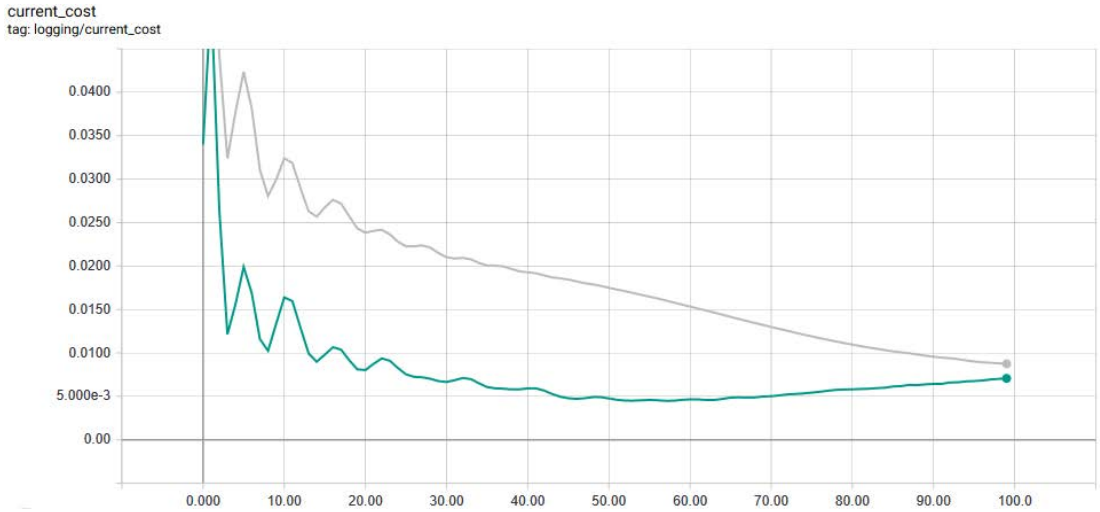
Şekil 4.9 : Eğitim ve sınama verilerinin maliyet grafiği.

Maliyet değerlerinin eğitim süreci devam ederken her adımda düştüğü ve yapay sinir ağlarının zaman içinde daha doğru sonuç verdiği görülmektedir. Üretilen son değerlerin görece birbirine yakın olması beklenmektedir. Ancak Şekil 4.9 incelendiğinde son maliyet değerlerinin birbirinden uzak olduğu görülmektedir.

Çizelge 4.4 : Model oluşturma sürecinde üretilen maliyet değerleri.

Durum İlerlemesi (Epoch)	Eğitim Maliyeti	Sınama Maliyeti
0	0.09991268813610077	0.08697476983070374
5	0.06188683956861496	0.03011937439441681
10	0.03627089783549309	0.011695434339344501
15	0.03640683740377426	0.018507400527596474
20	0.032410960644483566	0.014665888622403145
25	0.02998311072587967	0.01022004708647728
30	0.029340889304876328	0.00993947871029377
45	0.027320316061377525	0.010333939455449581
40	0.026598088443279266	0.010580625385046005
45	0.02541632018983364	0.00883098691701889
50	0.024681640788912773	0.008405154570937157
55	0.024044159799814224	0.00850766897201538
60	0.02332920767366886	0.007851709611713886
65	0.022671647369861603	0.007514228578656912
70	0.022050468251109123	0.007166221272200346
75	0.02134541980922222	0.007000967860221863
80	0.02057531662285328	0.006523133255541325
85	0.019790247082710266	0.0062268758192658424
90	0.018864845857024193	0.0057216365821659565
95	0.018088266253471375	0.005555667914450169
Toplam Son Durum	0.017429973930120468	0.005373946391046047

Şekil 4.10 ve Çizelge 4.5'de gizli katman sayısı 3 ve nöron sayısı 150 – 300 – 150 olan eğitilmiş modelinin sonuçları gösterilmektedir. Şekil üzerinde gri renk eğitim maliyetlerine, yeşil renk ise sınama maliyetlerine ilişkin grafiği göstermektedir.



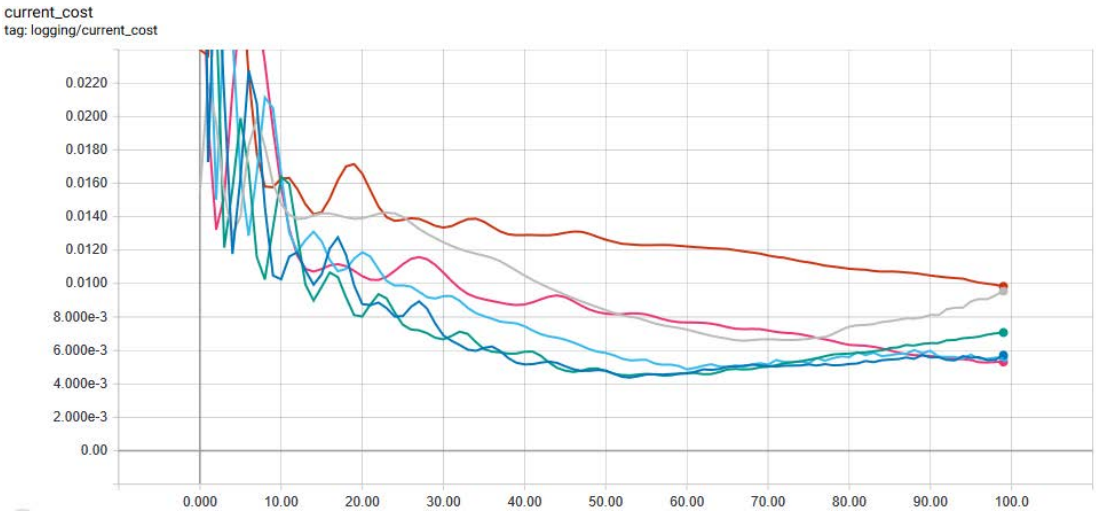
Şekil 4.10 : Eğitim ve sınama verilerinin maliyet grafiği.

Grafikte eğitme işlemi sonucunda değerlerin birbirine yaklaştığı ve nöron sayısı 150 – 300 – 150 olarak tanımlanan modelin daha iyi sonuç verdiği görülmektedir.

Çizelge 4.5 : Model oluşturma sürecinde üretilen maliyet değerleri.

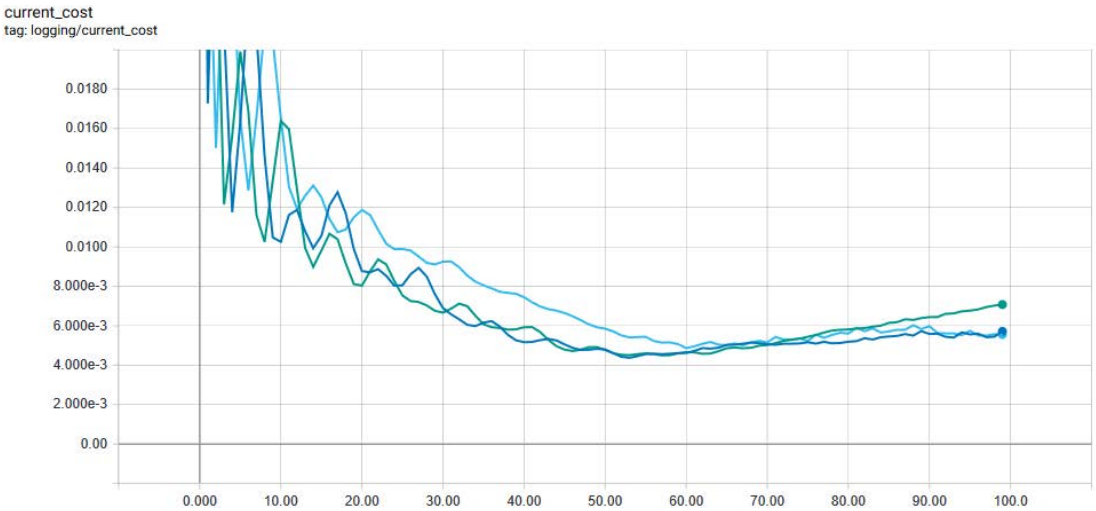
Durum İlerlemesi (Epoch)	Eğitim Maliyeti	Sınama Maliyeti
0	0.07289496809244156	0.06058710068464279
5	0.03018445149064064	0.012314089573919773
10	0.026517795398831367	0.012634335085749626
15	0.024808969348669052	0.011308366432785988
20	0.02288259007036686	0.010668158531188965
25	0.02142559364438057	0.00939324963837862
30	0.020213011652231216	0.009061390534043312
45	0.019225113093852997	0.008579744026064873
40	0.01820249855518341	0.007838832214474678
45	0.016987932845950127	0.007393191568553448
50	0.015735536813735962	0.006990613415837288
55	0.014371984638273716	0.006639665924012661
60	0.012972814030945301	0.006422728765755892
65	0.011773400008678436	0.00640864297747612
70	0.010793467052280903	0.006750587839633226
75	0.009955041110515594	0.007113431114703417
80	0.009336482733488083	0.0075425393879413605
85	0.008751343004405499	0.007475437596440315
90	0.008367737755179405	0.007322237826883793
95	0.008059614337980747	0.007553761824965477
Toplam Son Durum	0.007691083941608667	0.007341428659856319

Farklı nöron sayıları ile oluşturulmuş ve Şekil A.1'de gösterilen maliyet grafiklerinde yer alan sınama verilerine ilişkin grafikler sonuçların daha net karşılaştırılması amacıyla birleştirilmiş ve Şekil 4.11'de gösterilmiştir. Şekil üzerinde kırmızı renk 20-100-50, gri renk 100-400-20, koyu pembe renk 50-100-50, açık mavi renk 200-300-200, yeşil renk 150-300-150 ve koyu mavi renk 100-400-200 nöron değerlerine sahip modellerin sınama maliyetlerine ilişkin grafiğini göstermektedir.



Şekil 4.11 : 47 öznitelik içeren sınama verilerinin birleştirilmiş maliyet grafiği.

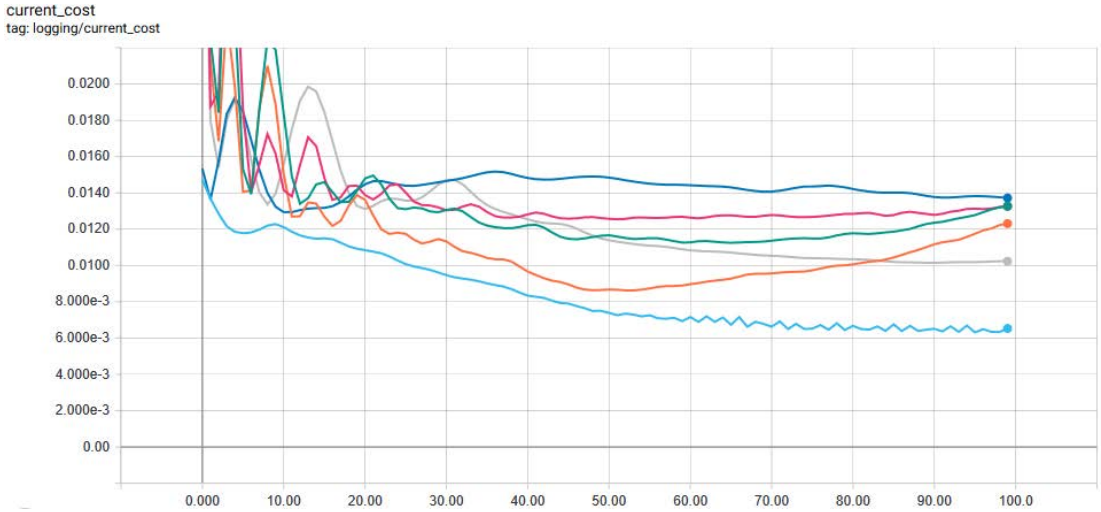
Sınama verilerine ilişkin maliyetler incelendiğinde 200-300-200, 150-300-150 ve 100-400-200 nöron değerlerine sahip modellerin diğerlerine göre daha iyi sonuç verdiği görülmektedir. Şekil 4.12'de ilerleme adımının 53 olduğu durumda 100-400-200 nöron değerlerine sahip modelin çok az farkla 150-300-150 nöron değerlerine sahip modelden daha iyi sonuç verdiği görülmektedir.



Şekil 4.12 : 47 özniteliğe ilişkin sınama verileri azaltılmış maliyet grafiği.

4.4.2 Çizelge A.2 ’de yer alan özniteliklerin kullanımıyla elde edilen sonuçlar

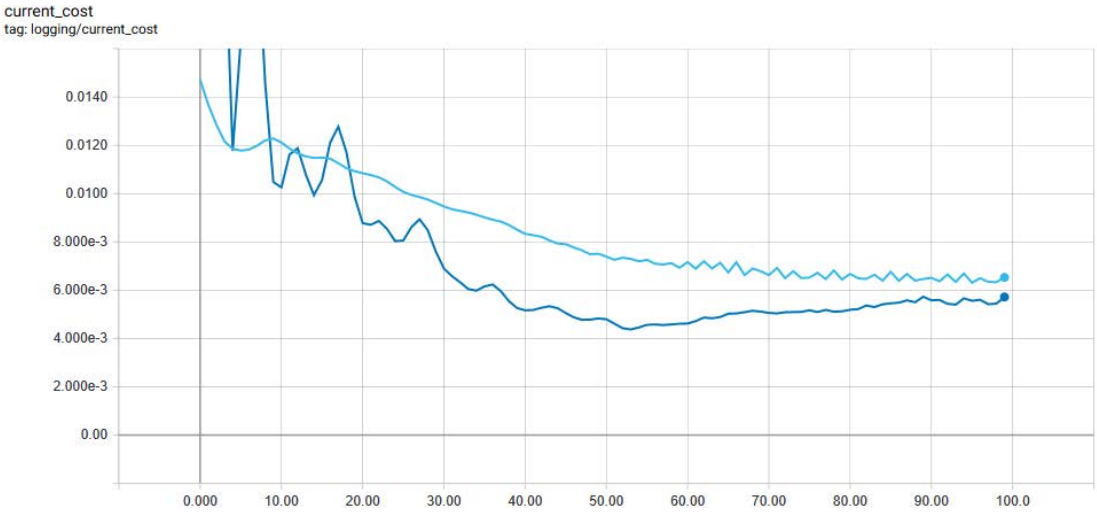
Şekil A.2’de, Çizelge A.3’te gösterilen 19 adet özniteliği içeren veri kümesi kullanılarak ve nöron sayısı değiştirilerek oluşturulan modeller için üretilmiş maliyet grafikleri yer almaktadır. Oluşturulan grafikler Şekil 4.13‘de gösterilmektedir. Şekil üzerinde koyu mavi renk 20-100-50, gri renk 50-100-50, koyu pembe renk 150-300-150, yeşil renk 100-400-200, turuncu renk 200-300-200 ve açık mavi renk 100-400-20 nöron değerlerine sahip modellerin sınama maliyetlerine ilişkin grafiğini göstermektedir.



Şekil 4.13 : 19 öznitelik içeren sınama verilerinin birleştirilmiş maliyet grafiği.

Grafik incelendiğinde 100-400-20 nöron değerlerine sahip modelin diğer modellere göre daha iyi sonuç verdiği görülmektedir.

Son aşamada 47 özniteliği içeren veri kümesi kullanılarak oluşturulmuş modellerden en iyi sonuç veren model ve öznitelik seçimi yapılarak oluşturulmuş 19 özniteliği içeren veri kümesi kullanılarak oluşturulmuş modellerden en iyi sonuç veren model karşılaştırılarak öznitelik seçiminin etkisi gözlemlenmiştir. Şekil 4.14'de sınama verilerine ilişkin maliyet grafiği gösterilmektedir. Şekil üzerinde açık mavi renk 19 özniteliğe sahip 100-400-20 nöron değerleri ile oluşturulmuş modeli, koyu mavi renk ise 47 özniteliğe sahip 100-400-200 nöron değerleri ile oluşturulmuş sınama verilerine ilişkin maliyet grafiğini göstermektedir. Grafik incelendiğinde 47 özniteliğe sahip modelin daha iyi sonuç verdiği görülmektedir. Bunun nedeni ise yapay sinir ağları algoritması kullanılarak model eğitme işlemi yapıldığında, algoritmanın her öznitelik için bir ağırlık tanımlaması ve bu tanımlanan ağırlıkların eğitim süresi boyunca tekrar tekrar güncellenmesi ve iyileştirilmesidir. Bu yaklaşım ile algoritma, karar verme sürecinde yardımcı olan özniteliklere daha yüksek değer vermekte ve kendisi için önemli olan öznitelikleri belirlemektedir.



Şekil 4.14 : 19 ve 47 özniteliklerine sahip sınama verilerinin maliyet grafiği.

5. SONUÇ VE ÖNERİLER

Saldırıların belirlenmesi kapsamında son dönemde yapılan çalışmalar ve yayımlanan teknik raporlar incelendiğinde kurum içi tehdit ve saldırıların daha büyük kayıplara neden olduğu belirtilmekte ve bu alandaki çalışmalara daha fazla önem verilmesi gerektiği ifade edilmektedir. Bu nedenle tez çalışması kapsamında kurum ya da kuruluş içindeki olağan dışı durumların veya saldırıların belirlenmesi konusuna odaklanılmıştır.

5.1 Yürütülen Çalışma

Çalışma kapsamında kurum ya da kuruluş içinde olabilecek tehdit ve saldırılar incelenmiş ve bu saldırılardan korunmak için alınabilecek önlemler açıklanmıştır. Ayrıca saldırıların belirlenmesi ve önlenmesi konusunda geliştirilen sistemlere katkı sağlanması adına Ağ Davranışlarında Olağan Dışı Durumların Belirlenmesi (NBAD) yaklaşımı ile ağın olağan davranış modelinin oluşturulmuş ve ağ üzerinde oluşan yeni, bilinmeyen ve olağan dışı durum ve saldırıların belirlenmesi amaçlanmıştır.

Bu sistemin kurulabilmesi ve işletilebilmesi amacıyla derin öğrenme yaklaşımının temelini oluşturan yapay sinir ağları algoritması kullanılmış ve UNB ISCX IDS 2012 veri kümesi ile model eğitimi gerçekleştirilmiştir. Oluşturulan model üzerinde sınama verilerinin öngörü değerleri incelenmiş ve %98.44 oranında doğruluk elde edilmiştir.

5.2 İleriki Çalışmalar

Makine öğrenmesi dünyasında modele dayanarak karar veren sistemler için en önemli kavram veridir. Verilerin çeşitli ve anlamlı olması daha doğru kararların üretilmesine olanak tanımaktadır. Bu kapsamda verilerin çeşitlendirilmesi yani sentetik verilerin üretilmesi geleceğin çalışma konuları arasında yer almaktadır. Diğer devam eden bir çalışma alanı ise davranışların modellenmesi hususunda anlık grafiklerin oluşturulması ve davranış modellerinin görüntü tanıma ile belirlenmesidir.

KAYNAKLAR

[1] **Adalı, E.** (2016): Bilgisayar ve Bilgi Güvenliği ve Yönetimi. İTU Ulusal Sertifikasyon Merkezi.

[2] **Marais, P., and Ostwalt, P.,** 2016: Global profiles of the fraudster: Technology enables and weak controls fuel the fraud. KPMG International Technical Report.

[3] **Clearswift,** 2015: Clearswift Insider Threat Index. RUAG Cyber Security Technical Report, US Edition.

[4] **Bandyopadhyay, S. K.,** 2008: Implementing intrusion detection system by considering insider attacks. Journal of Security Engineering, vol. 15, no.4, pp. 295-302.

[5] **Li, T., and Horkoff, J.,** 2014: Dealing with security requirements for sociotechnical systems: A holistic approach. Advanced Information Systems Engineering (CAiSE 2014). Springer International Publishing, pp. 285-300.

[6] **Barnum, S., and Sethi, A.,** 2007: Attack patterns as a knowledge resource for building secure software. OMG Software Assurance Workshop: Cigital, 2007.

[7] **Lamsweerde, A. V.,** 2004: Elaborating security requirements by construction of intentional anti-models. Proceedings of the 26th International Conference on Software Engineering (ICSE, 2004), pp. 148-157.

[8] **Sindre, G., and Opdahl, A. L.,** 2005: Eliciting security requirements with misuse cases. Requirements Engineering, vol. 10, no. 1, pp. 34-44.

[9] **Li, T., Paja, E., Mylopoulos, J., Horkoff, J., and Beckers, K.,** 2015: Holistic security requirements analysis: An attacker's perspective. Requirements Engineering Conference (RE), 2015, pp. 282-283.

[10] **Moore, A. P., Ellison, R. J., and Linger, R. C.,** 2001: Attack modeling for information security and survivability. CMU-SEI-2001-TN-001, Technical Report.

[11] **Url-1** <*http://capec.mitre.org*>, alındığı tarih: 11.09.2018.

[12] **Li, T., Horkoff, J., Beckers, K., Paja, E., and Mylopoulos, J.,** 2015: A holistic approach to security attack modeling and analysis. Proceedings of the 8th International iStar Workshop, pp. 49-54.

[13] **Li, T., Horkoff, J., Beckers, K., Paja, E., and Mylopoulos, J.,** 2015: Analyzing attack strategies through anti-goal refinement. The Practice of Enterprise Modeling (PoEM). Springer International Publishing, pp. 75-90.

[14] **Li, T., Paja, E., Mylopoulos, J., Horkoff, J., and Beckers, K.,** 2016: Security attack analysis using attack patterns. IEEE 10th International Conference on Research Challenges in Information Science (RCIS), Grenoble, France, June 1-3.

[15] **Ali, R., Dalpiaz, F., and Giorgini, P.,** 2010: A goal-based framework for contextual requirements modeling and analysis. Requirements Engineering, vol. 15, no. 4, pp. 439-458.

[16] **Shostack, A.,** (2014): Threat Modeling: Designing for Security. John Wiley & Sons.

[17] **Kabiri, P., and Goharbani, A. A.,** 2005: Research in intrusion detection and response: A survey. International Journal of Network Security, vol. 1, no. 2, pp. 84-102.

[18] **Sobh, T. S.,** 2006: Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces, pp. 670-694.

[19] **Denning, E. D.,** 1987: An intrusion-detection model. IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222–232.

[20] **Staniford-Chen S., Tung B., Porrar P., Kahn C., Schnackenberg D., Feiertag R.,** et al. 1998: The common intrusion detection framework data formats. Internet draft, 'draft-staniford-cidf-dataformats- 00.txt'.

[21] **Garcia-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., and Vázquez, E.,** 2009: Anomaly-based network intrusion detection: Techniques, systems and challenges. Computer and Security, vol. 28, no. 1-2, pp. 18-28.

[22] **Li, X., Meng, J., Zhao, H., and Zhao, J.,** 2015: Overview of Intrusion Detection Systems. Journal of Applied Science and Engineering Innovation, vol. 2, no. 6, pp. 230-232.

[23] **Url-2** <*https://tools.ietf.org/html/rfc4767*>, alındığı tarih: 12.10.2018.

[24] **Url-3** <*https://tools.ietf.org/html/rfc4765*>, alındığı tarih: 12.10.2018.

[25] **Url-4** <*https://tools.ietf.org/html/draft-ietf-idwg-iap-01*>, alındığı tarih: 12.10.2018.

[26] **Tylman, W.,** 2008: Misuse-based intrusion detection using Bayesian networks. International Journal of Critical Computer-Based Systems, vol. 1, no. 1, pp. 178-190.

[27] **Villar, F., Goc, M. L., Bouche, P., and Rolland, P.,** 2015: Discovering internal fraud models in a stream of banking transactions. 7th International Joint Conference on Computational Intelligence (IJCCI), Lisbon, Portugal, November 12-14.

[28] **Kakuru, S.,** 2011: Behavior based network traffic analysis tool. 3rd International Conference on Communication Software and Networks, Xi'an, China, May 27-29.

[29] **Han, M., and Kim, I.,** 2015: Anomaly detection method using network pattern analysis of process. 2015 World Congress on Internet Security (WorldCIS), Dublin, Ireland, October 19-21.

[30] **Garcia, S.,** 2015: Modelling the network behaviour of malware to block malicious patterns. The stratosphere project: A behavioural IPS. VirusBulletin Conference, Prague, Czech Republic.

[31] **Schulze, H.,** 2018: Insider threat report. CA Technologies.

[32] **Stolfo, S.J., Bellovin, S. M., Hershkop, S., Keromytis, A. D., Sinclair, S., and Smith, S.,** (2008): Insider Attack and Cyber Security: Beyond the Hacker. Springer.

[33] **Url-5** <*https://cve.mitre.org*>, alındığı tarih: 02.11.2018.

[34] **Este´vez-Tapiador, J. M., Garcı´a-Teodoro, P., and Dı´az-Verdejo, J. E.,** 2003: Stochastic protocol modeling for anomaly based network intrusion detection. In: Proceedings of IWIA 2003. IEEE Press, ISBN 0-7695-1886-9, pp. 3-12.

[35] **Lazarevic, A., Kumar, V., and Srivastava, J.,** (2005): Intrusion detection: A survey, Managing cyber threats: issues, approaches, and challenges. Springer Verlag, pp. 19-78.

[36] **Denning, D. E., and Neumann, P. G.,** 1985: Requirements and model for IDES - A real-time intrusion-detection expert system. Final Report, SRI International.

[37] **Ye, N., Emran, S. M., Chen, Q., and Vilbert, S.,** 2002: Multivariate statistical analysis of audit trails for host-based intrusion detection. IEEE Transactions on Computers, vol. 51, no. 7, pp. 810-820.

[38] **Anderson, D., Lunt, T. F., Javitz, H., Tamaru, A., and Valdes, A.,** 1995: Detecting unusual program behaviour using the statistical component of the next-generation intrusion detection expert system (NIDES). Menlo Park, CA, USA: Computer Science Laboratory, SRI International; 1995. SRIO-CSL-95-06.

[39] **Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., and Zhou, S.,** 2002: Specification-based anomaly detection: A new approach for detecting network intrusions. CCS '02 Proceedings of the 9th ACM conference on Computer and communications security, pp. 265-274.

[40] **Hopfield, J. J.,** 1988: Artificial neural networks. IEEE Circuits and Devices Magazine, vol. 4, no. 5, pp. 3-10.

[41] **McClelland, J. L., Rumelhart, D. E., and Hinton, G. E.,** (1986): The appeal of parallel distributed processing. Cognitive Psychlogy, MIT Press, vol. 1, pp. 3-44.

[42] **Abrahart, R. J., and See, L.,** 2011: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security, vol. 31, no. 3, pp. 357-374.

[43] **Url-6** <*https://unb.ca/cic/datasets/*>, alındığı tarih: 02.11.2018.

[44] **Url-7** <*https://wireshark.org*>, alındığı tarih: 02.11.2018.

[45] **Adalı, E., and Gül, A.,** 2017: A feature selection algorithm for IDS. International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, October 5-8.

[46] **Url-8** <*https://scikit-learn.org/stable/modules/preprocessing.html*>, alındığı tarih: 02.11.2018.

[47] **Url-9** <*https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html*>, alındığı tarih: 02.11.2018.

[48] **Url-10** <*https://www.tensorflow.org*>, alındığı tarih: 02.11.2018.

[49] **Url-11** <*https://www.nvidia.com/en-sg/data-center/gpu-accelerated-applications/tensorflow/*>, alındığı tarih: 02.11.2018.

[50] **Url-12** <*https:// colab.research.google.com*>, alındığı tarih: 02.11.2018.

EKLER

EK A.1: .pcap uzantılı dosyalardan çıkarılan veri türleri tablosu
EK A.2: Öğrenme algoritmasında kullanılan öznitelikler
EK A.3: Önemi yüksek öznitelikler
EK A.4: Sözlük
EK A.5: 1 adet yazılım CD'si

EK A.1

Çizelge A.1 : Pcap dosyasından çıkarılan veri türleri.

frame.number	frame.time_epoch	col.UTCDateTime	frame.len
_ws.col.Protocol	arp	ip.src	ip.dst
ip.version	ip.proto	ip.flags.mf	ip.ttl
icmp	icmpv6	dhcpv6	igmp
udp.stream	udp.srcport	udp.dstport	tcp.stream
tcp.srcport	tcp.dstport	tcp.flags.ack	tcp.flags.push
tcp.flags.reset	tcp.flags.syn	tcp.flags.fin	tcp.analysis. duplicate_ack
tcp.analysis. retransmission	tcp.analysis. fast_ retransmission	tcp.analysis.spurious _retransmission	tcp.analysis. out_of_order
tcp.analysis. zero_window	tcp.analysis. keep_alive	tcp.analysis. ack_rtt	tcp.analysis .reused_ports
http	http.request	http.response	http.response.code
http. leading_crlf	pop	pop.response. indicator	smtp
smtp.response. code	imap	imap.line	dns
dns.qry.type	dns.flags.response	dns.flags.rcode	dns.retransmission
dns.retransmit_ request	dns.retransmit_ response	nbns	nbns.flags.broadcast
nbns.flags. response	nbns.flags.rcode	mdns	llmnr
ssh	ftp	ftp.request	ftp.request.command
ftp.response	ftp.response.code	ftp.response. code.invalid	nbss
nbss.type	smb	lanman	browser
browser. server_ type. workstation	browser. server_type. server	browser.server_ type.sql	browser. server_type. browser.master
browser. server_type. Browser .potential frame.number	frame. time_epoch	ip.src	frame.len

EK A.2

Çizelge A.2 : Öğrenme algoritmasında kullanılan öznitelikler.

Label	srcIPField1	srcIPField2	srcIPField3
srcIPField4	dstIPField1	dstIPField2	dstIPField3
dstIPField4	srcPort	dstPort	isTCP
isUDP	ICMP	TcpFlagAck	TcpFlagRst
TcpFlagSyn	TcpFlagFin	TcpFlagPush	IGMP
Msnms	Llmnr	HTTP	SSH
POP	SMTP	IMAP	ARP
NBSS	DNS	NetBios	MSN
Duration	ICMP	FTP	WebMediaDocuments
NTP	MSB	HTTPS	WebMediaAudio
Broadcast	Unknown Udp	Unknown Tcp	dstPacketNumber
srcPacketByte	srcPacketNumber	dstPacketByte	MiscApplication

EK A.3

Çizelge A.3 : Önemi yüksek öznitelikler.

Label	srcIPField2	srcIPField3	srcIPField4
dstIPField1	dstIPField2	dstIPField3	dstIPField4
srcPort	dstPort	dstPacketByte	srcPacketNumber
duration	UnknownTcp	srcPacketByte	srcTcpFlagsSyn
srcTcpFlagsAck	srcTcpFlagsPush	srcTcpFlagsFin	dstTcpFlagsAck

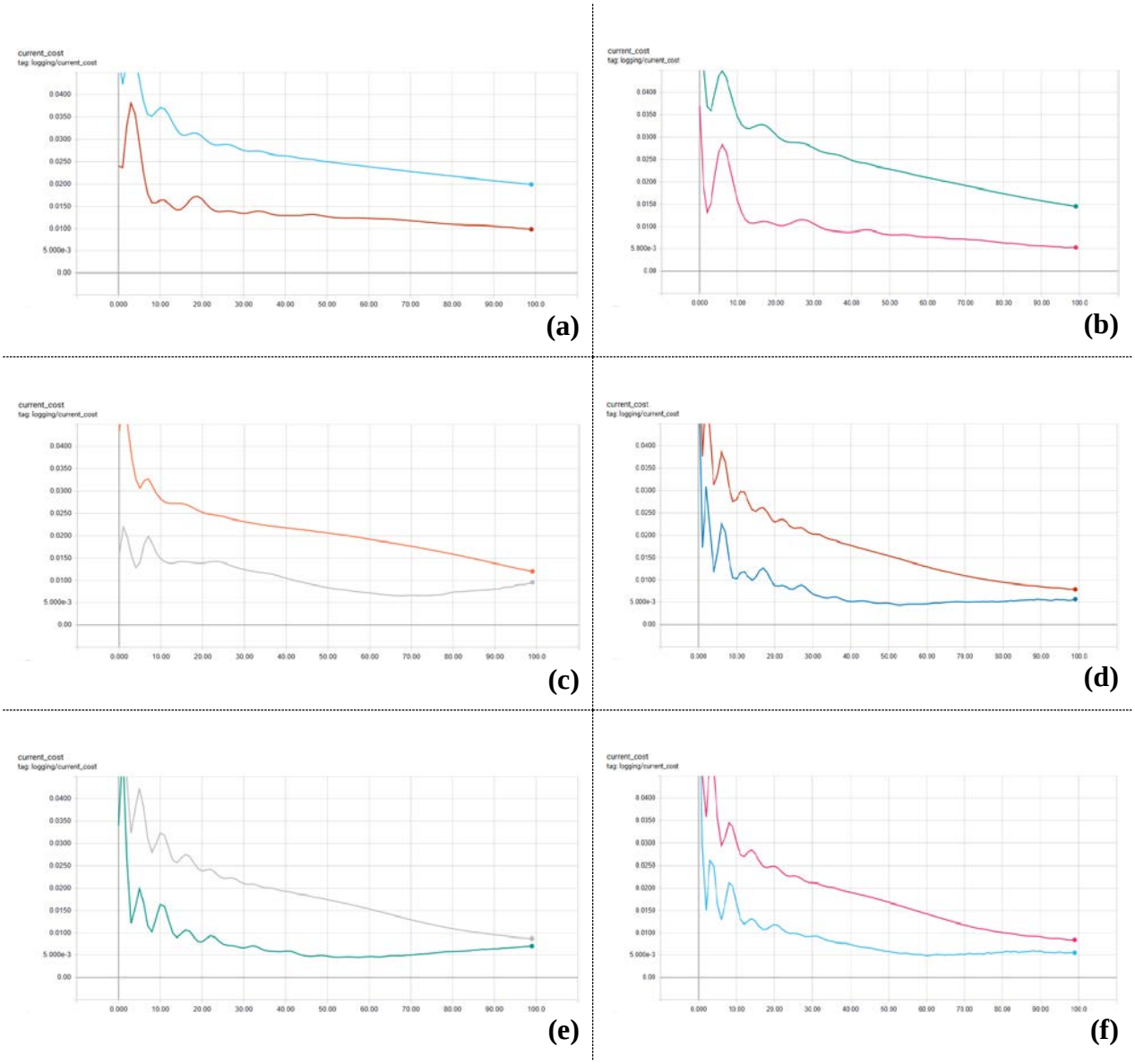
EK A.4

Çizelge A.4 : Sözlük.

Türkçe	İngilizce
Ağ Davranış Çözümlemesi	Network Behavioral Analysis
Anahtar	Switch
Bağdaşma	Correlation
Belirtim Temelli Olağan Dışı Durum Belirleme	Specification-based Anomaly Detection
Beyaz ve kara liste	White and black list
Bilgi Tabanlı Yaklaşım	Knowledge-based Techniques
Bütünlük	Integrity
Çapraz doğrulama ile yinelemeli öznitelik eleme	Recursive feature elimination with cross validation
Çizge temelli yöntemler	Graph-based methods
Çoğaltma varsayımı	Manifold assumption
Çok değişkenli modeller	Multivariate models
Değişkenlere ayırma	Parametrization
Denetimli Makine Öğrenmesi	Supervised Machine Learning
Denetimsiz Makine Öğrenmesi	Unsupervised Machine Learning
Durum ilerlemesi	Epoch
Düşük yoğunluk ayrımı	Low-density separation
Erişilebilirlik	Availability
Gauss rasgele değişkenler	Gaussian random variables
Gelişmiş Sürekli Tehdit	Advanced Persistent Threats
Gizlilik	Confidentiality
Gökkuşağı çizelgesi ile parolayı çözme	Rainbow table password cracking
Grafik haritası	Heatmap
Hedef	Target
Hedef modelleme tekniği	Goal modeling technique
İmza temelli saldırı belirleme	Signature-based detection
İskele	Port
Kaba kuvvet	Brute force
Karşıt-hedef analizi	Anti-goal analysis
Kimlik doğrulamayı atlama	Authentication bypass
Komuta kontrol kanalları	Command and control (C&C) channel
Kötü amaçlı yazılım	Malware
Kötüye kullanım	Misuse case
Kurum içi tehdit	Insider Threat
Kurum içi saldırı	Insider Attack
Kümeleme varsayımı	Cluster assumption
K-ortalama algoritması	K-means algorithm
Maliyet	Cost
Maymuncuk	Lock picking
Olağan dışı durum temelli saldırı belirleme	Anomaly-based intrusion detection
Öngörülen değer	Prediction value

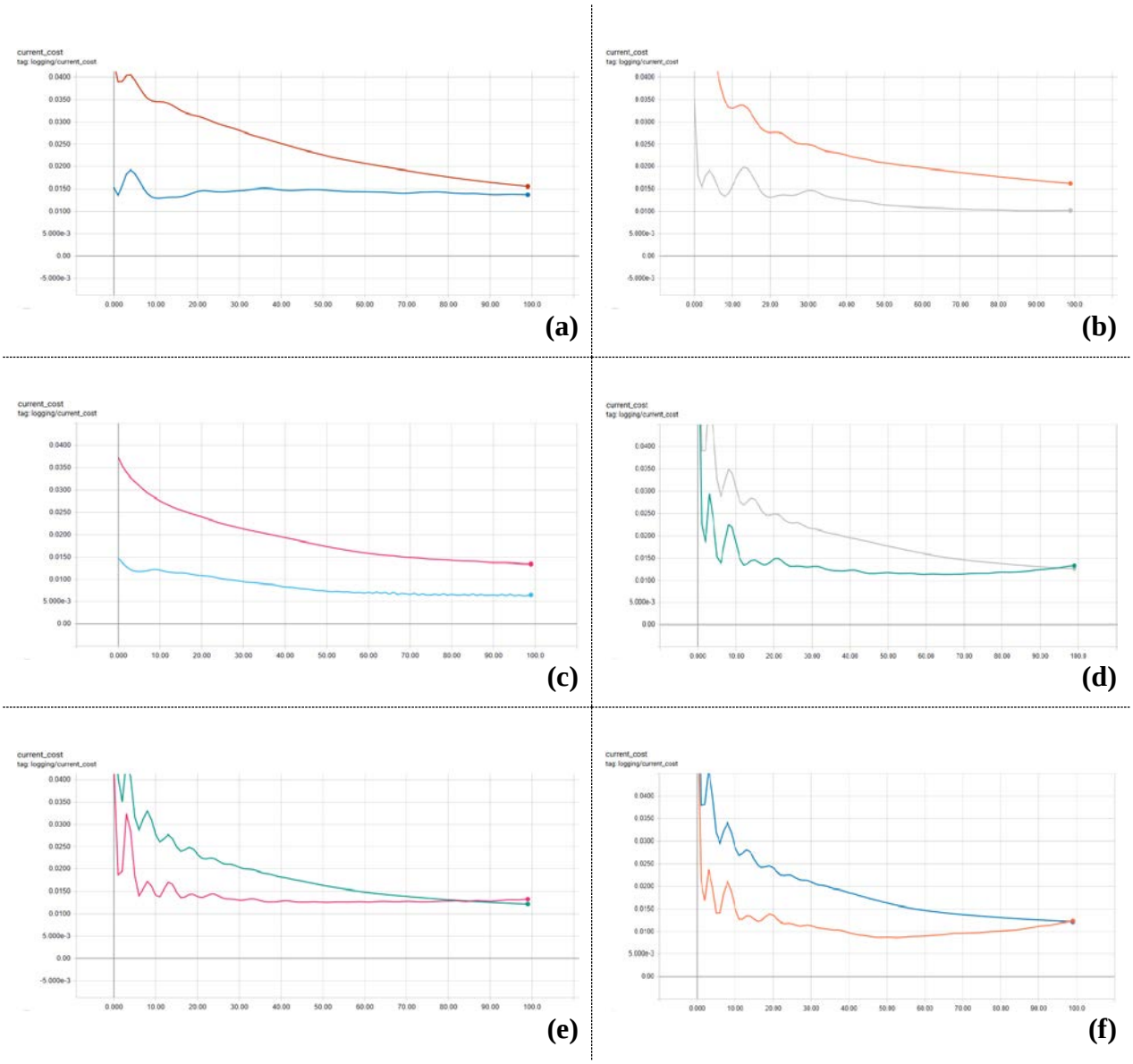
Öznitelik Çıkarımı	Feature Extraction
Öznitelik Seçimi	Feature Selection
Paket Dinleyicisi	Packet sniffer
Parmak izleri	Fingerprints
Saldırı	Attack
Saldırı Belirleme	Intrusion Detection
Saldırı modelleri	Attack patterns
Sezgisel yaklaşımlar	Heuristic approaches
Sıfır Gün	Zero Day
Sözlük temelli şifre saldırısı	Dictionary based password attack
Süreklilik varsayımı	Continuity assumption
Tehdit	Threat
Tek değişkenli modeller	Univariate models
Tek değişkenli öznitelik seçimi	Univariate feature selection
Uygulama Erişilebilirliği	Application Availability
Üretici modeler	Generative models
Varlık	Asset
Veri Gizliliği	Data Confidentiality
Yapay Sinir Ağları	Artificial Neural Network
Yarı Denetimli Makine Öğrenmesi	Semi-supervised Machine Learning
Yetki	Authorization
Yinelemeli öznitelik eleme	Recursive feature elimination
Yığın kaynaklı tehdit istihbaratı analizi	Crowd-sourced threat intelligence analytics
Yönlendirici	Router

EK A.5



Şekil A.1 : 47 öznitelik ve farklı gizli nöron sayıları ile üretilen maliyet grafikleri: (a)20-100-50. (b)50-100-50. (c)100-400-20. (d)100-400-200. (e)150-300-150. (f)200-300-200.

EK A.6



Şekil A.2 : 19 öznitelik ve farklı gizli nöron sayıları ile üretilen maliyet grafikleri: (a)20-100-50. (b)50-100-50. (c)100-400-20. (d)100-400-200. (e)150-300-150. (f)200-300-200.

ÖZGEÇMİŞ

Ad Soyad: Ayşe GÜL

Doğum Yeri ve Tarihi: Üsküdar, 02.01.1991

Adres: 34912, Pendik, İstanbul

E-Posta: gula16@itu.edu.tr

Lisans: İstanbul Üniversitesi

Mesleki Deneyim ve Ödüller:

- (Aralık 2014 – Devam Ediyor) Havelsan / Yazılım Geliştirme Mühendisi
- (Eylül 2014 – Aralık 2014) Solvoyo / Yazılım Mühendisi

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR

- **Gül, A.,** and Adalı, E., 2017: A feature selection algorithm for an IDS, International Conference on Computer Science and Engineering (UBMK), October 3-8, Antalya, Turkey.