AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ
YÜKSƏK TƏHSİL İNSTİTUTU

Əlyazması hüququnda

Aytən Hüseynova Elçin qızı
Elnur İbrahimov Eldəniz oğlu
Qiyas Cəfərov Rauf oğlu
Səməd Cabbarlı Sidqi oğlu
Vüqar Stanbullu Dərgah oğlu

KOMPÜTER ŞƏBƏKƏLƏRİNİN KİBERTƏHLÜKƏSİZLİYİNİN MONİTORİNQİNƏ SÜNİ İNTELLEKT TEXNOLOGİYALARININ TƏTBİQİ

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

060632 – "İnformasiya texnologiyaları və sistemləri mühəndisliyi"

6063212 – "Kibertəhlükəsizlik (SABAH)"

Elmi rəhbər: _____ tex.f.d., dos. Ramiz Şıxəliyev.

BAKI-2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ
YÜKSƏK TƏHSİL İNSTİTUTU

MAGİSTRANTIN ANDI

Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinə süni intellekt texnologiyalarının tətbiqi mövzusunda təqdim etdiyimiz magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayət etməklə və istifadə etdiyimiz bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığımıza and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya Mərkəzində saxlanılması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

Aytən Hüseynova
Elnur İbrahimov
Qiyas Cəfərov
Səməd Cabbarlı
Vüqar Stanbullu

Tarix

XÜLASƏ

İşin adı: Kompüter Şəbəkələrinin Kibertəhlükəsizliyinin Monitorinqinə Süni İntellekt Texnologiyalarının Tətbiqi

Bu magistr dissertasiya işində kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinə süni intellekt texnologiyalarının tətbiqi ilə bağlı məsələlər müzakirə olunmuşdur və əsas diqqət maşın təlimi və dərin təlim üsulları istifadəsi ilə modellərin yaradılmasına yetirilir. İşdə qarşıya qoyulmuş bir neçə məsələ istiqamətində tədqiqatlar aparılmaqla aşağıdakı nəticələrlə yekunlaşmışdır:

- Kompüter şəbəkələrinin kibertəhlükəsizliyi və mövcud monitorinq texnologiyaları analiz edilmişdir.
- Süni intellektin əsas üsulları və onların kibertəhlükəsizlikdə tətbiqi analiz edilmişdir.
- Kompüter şəbəkələrində müdaxilələrin dərin təlim əsasında aşkarlanması modeli işlənilmişdir.
- Kompüter şəbəkələrində anomaliyaların maşın təlimi əsasında aşkarlanması modeli işlənilmişdir.
- Kompüter şəbəkələrində zərərli proqramların dərin təlim əsasında aşkarlanması modeli işlənilmişdir.
- İşlənmiş modellərin effektivliyinin və dəqiqliyinin qiymətləndirməsi üçün açıq verilənlər dəsti üzərində eksperimental analiz aparılmışdır.

SUMMARY

Title of work: Application of Artificial Intelligence Technologies to Cyber Security Monitoring of Computer Networks

In this master's thesis, issues related to the application of artificial intelligence technologies to the monitoring of cyber security of computer networks are discussed, and the main focus is on the creation of models using machine learning and deep learning methods. Researches were carried out in the direction of several issues and concluded with the following results:

- Cyber security of computer networks and existing monitoring technologies were analyzed.
- The main methods of artificial intelligence and their application in cyber security were analyzed.
- A model for detection of intrusions in computer networks based on deep learning was developed.
- A model for detecting anomalies in computer networks based on machine learning was developed.
- A model for detection of malicious programs in computer networks based on deep learning has been developed.
- An experimental analysis was conducted on an open data set to evaluate the effectiveness and accuracy of the developed models.

Mündəricat

İXTİSARLARIN SİYAHISI

CNN	Convolutional Neural Network	Konvolyusiya Neyron Şəbəkəsi
DDOS	Distributed Denial of Service	Paylanmış xidmətdən imtina
DL	Deep Learning	Dərin Təlim
DOS	Denial of Service	Xidmətdən imtina
GRU	Gated Recurrent Unit	Qapalı təkrarlanan blok
LSTM	Long short-term memory	Uzun qısamüddətli yaddaş
MITM	Man-in-the-middle	Ortadakı Adam
NTA	Network Traffic Analysis	Şəbəkə trafikinin təhlili
RNN	Recurrent Neural Network	Təkrarlanan Neyron Şəbəkəsi
SCA	Side-chanel Analysis	Yan Kanal Təhlili
SIEM	Security Information and Event Management	Təhlükəsizlik Məlumatlarının və Hadisələrinin İdarəsi
SOM	Self-organizing Map	Özünü təşkil edən xəritə
SQL	Structured query language	Strukturlaşdırılmış Sorğu Dili

GİRİŞ

Mövzunun aktuallığı: Təşkilatların və dövlət qurumlarının fəaliyyətində kompüter şəbəkələrinin əsas rol oynadığı müasir informasiya cəmiyyətində kibertəhlükəsizliyin təmin edilməsi prioritet məsələdir. Mürəkkəb kiberhücumların sayının çoxalması real vaxt rejimində təhdidləri aşkar etmək və yumşaltmaq qabiliyyətinə malik güclü monitorinq sistemlərinin yaradılmasını zəruri etmişdir.

Kompüter şəbəkəsi kompüter sistemləri, terminal və periferik avadanlıqlar arasında verilənlərin ötürülməsinə imkan verən, bir-biri ilə qarşılıqlı əlaqədə olan verilənlərin ötürülməsi sistemlərinin məcmusudur (ISO/IEC, 2015)

Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqi informasiya sistemlərinin təhlükəsizliyinin təmin edilməsində və kibertəhlükələrdən müdafiənin əsas komponentidir və təhdidlərin çevik aşkarlanması və cavablandırılmasının təmin edilməsində mühüm rol oynayır. Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqi kibertəhlükələrin və hücumların aşkar edilməsi, analizi və qarşısının alınması məqsədilə kompüter şəbəkələrinin vəziyyətinin və fəaliyyətinin sistematik şəkildə monitorinqi prosesidir. O, şəbəkə trafikinin monitorinqi, təhlükəsizlik hadisələrinin təhlili, anomaliyaların aşkarlanması, təhlükənin idarə edilməsi, audit və s. kimi müxtəlif aspektlərə malikdir.

Kompüter şəbəkələrinin kibertəhlükəsizliyin monitorinqinin hazırkı vəziyyəti bir sıra əsas xüsusiyyətlər və tendensiyalarla xarakterizə olunur. Kompüter şəbəkələrində avadanlıqların və xidmətlərin sayının davamlı artması ilə kiber təhlükələrin aşkar edilməsi üçün analiz edilməli olan informasiyanın həcmi artır (J. Camacho, G. Maciá-Fernández, J.E.D. Verdejo and P. García-Teodoro, 2014). Bu, anomaliya fəaliyyətlərin effektiv şəkildə izlənilməsi və müəyyən edilməsi üçün verilənlərin yeni emal üsullarından və texnologiyalarından, xüsusi ilə verilənlərin analitikasından istifadəni zəruri edir.

Kibertəhlükələr getdikcə daha çox artır və mürəkkəbləşir, tez-tez hədəflərə koordinasiyalı hücumlar edilməsi üçün botnetlərdən və digər vasitələrdən istifadə

edilir. Bu, hücumların dinamik təbiətinə uyğunlaşa bilən və onlara tez cavab verə bilən aşkarlama və müdafiə üsullarının işlənilməsini tələb edir.

Kibercinayətkarlar həssas məlumatlara çıxış əldə etmək üçün getdikcə daha çox sosial mühəndislik və fişinq üsullarından istifadə edirlər. Beləliklə, kibertəhlükəsizliyin monitorinqinin hazırkı vəziyyəti texnologiya və texnikanın sürətli inkişafı, eləcə də kibertəhdidlərin daim təkamülü ilə xarakterizə olunur. Buna görə də, kibertəhlükəsizliyin təmin edilməsi üçün ən son üsul və texnologiyalardan istifadə tələb olunur. Bu kontekstdə kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqi üçün süni intellekt texnologiyalarının istifadəsi zərurətə çevrilir.

Son onilliklər ərzində dərin təlim, neyron şəbəkələri, konvolyusiya neyron şəbəkələri, maşın təlimi və s. kimi bir çox yeni süni intellekt üsulları ortaya çıxmışdır. Bu üsullar verilənlərdən bilik əldə etməyə və proqnozlar verməyə imkan verir və böyük həcmdə verilənlərin analizi və gizli nümunələrin müəyyən edilməsi əsasında naməlum təhdidləri və anomaliyaları aşkarlaya bilir. Maşın təlimi (MT) və dərin təlim (DT) kimi yeni süni intellekt üsullarının meydana çıxması ilə daha dəqiq və effektiv kibertəhlükəsizlik monitorinq sistemlərini yaratmaq mümkün olmuşdur.

Kompüter şəbəkələrinin kibertəhlükəsizliyin monitorinqində süni intellektin istifadəsi kiberhücumların aşkarlanması və qarşısının alınmasında əsas rol oynayır və kompüter şəbəkələrinin kibertəhlükəsizliyinin təmin edilməsi istiqamətində tədbirlərin səmərəliliyini artırmağa, insidentlərə cavab müddətini azaltmağa və kiberhücumlardan dəyən zərəri minimuma endirməyə imkan verir.

Anomaliyaların aşkarlanması üçün MT alqoritmlərinin istifadəsi kompüter şəbəkələrinə potensial kiberhücumların və ya qeyri-adi davranışın aşkarlanması əsasında təhlükəsizlik pozuntularını avtomatik müəyyən edə bilər.

MT modelləri yeni kibertəhlükələrin ehtimalını proqnozlaşdırmaq və ən çox ehtimal olunan kiberhücum ssenarilərini müəyyən etmək üçün kiberhücumlar və onların xüsusiyyətləri haqqında böyük həcmdə məlumatları analiz edə bilər. MT alqoritmləri mürəkkəb kiberhücum ssenarilərini analiz etməyə və onların qarşısını almaq və ya məhdudlaşdırmaq üçün ağıllı həllər təqdim etməyə kömək edə bilər.

Süni intellekt sistemləri aşkar edilmiş təhdid və kiberhücumlara avtomatik cavab verə bilər, məsələn, girişi bloklamaq və ya yoluxmuş sistemləri təcrid etməklə zərəri minimuma endirə bilər. Süni intellekt şəbəkə trafiki, audit jurnalları və təhlükəsizlik hadisələri də daxil olmaqla böyük həcmdə məlumatları analiz edə bilər ki, bu da ona hadisələr arasında qanunauyğunluqları və əlaqələri müəyyən etməyə imkan verir. Süni intellekt sistemləri yeni kibertəhdid növlərinə və dəyişən şəraitə uyğunlaşaraq, daim dəyişən kibertəhlükələrin öhdəsindən effektiv şəkildə gəlməyə imkan verə bilər.

Tədqiqatın məqsədi və məsələləri: Dissertasiya işinin məqsədi kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqi üçün süni intellekt texnologiyalarından istifadənin araşdırılması və monitorinq modellərinin işlənilməsidir.

Bu məqsədə çatmaq üçün aşağıdakı vəzifələr müəyyən edilmişdir:

➢ Kompüter şəbəkələrinin kibertəhlükəsizliyi və mövcud monitorinq texnologiyalarının analizi.

➢ Süni intellektin əsas üsullarının və onların kibertəhlükəsizlikdə tətbiqinin analizi.

➢ Kompüter şəbəkələrində müdaxilələrin dərin təlim əsasında aşkarlanması modelinin işlənilməsi.

➢ Kompüter şəbəkələrində anomaliyaların maşın təlimi əsasında aşkarlanması modelinin işlənilməsi.

➢ Kompüter şəbəkələrində zərərli proqramların dərin təlim əsasında aşkarlanması modelinin işlənilməsi.

➢ İşlənmiş modellərin effektivliyinin və dəqiqliyinin qiymətləndirməsi üçün açıq verilənlər dəsti üzərində eksperimental tədqiqi.

Tədqiqatın metodikası və obyekti: Tədqiqatın obyekti kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinə süni intellekt texnologiyalarının tətbiqidir. Tədqiqatın predmeti kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinin

mövcud yanaşmalarının və süni intellekt texnologiyalarının analizi, həmçinin süni intellekt üsulları əsasında modellərin işlənilməsidir.

Mövcud ədəbiyyat əsasında kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqin yanaşmaları, maşın təlimi və dərin təlim üsullarının analitik icmalı aparılmışdır. Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinə süni intellekt texnologiyalarının tətbiqi məsələləri analiz edilmişdir. Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqi üçün MT və DT üsullarının əsasında modellər işlənilmişdir və onların effektivliyinin və dəqiqliyinin qiymətləndirməsi üçün açıq verilənlər dəsti üzərində eksperimentlər aparılmışdır.

Tədqiqatın elmi yeniliyi və praktik əhəmiyyəti. Tədqiqatın elmi yeniliyi kimi aşağıdakıları qeyd etmək olar:

➢ Kompüter şəbəkələrinin kibertəhlükəsizliyi və monitorinq texnologiyaları analiz edilmişdir;

➢ Süni intellektin əsas üsulları və onların kibertəhlükəsizlikdə tətbiqi məsələləri analiz edilmişdir;

➢ Kompüter şəbəkələrində müdaxilələrin aşkarlanması üçün dərin təlim əsasında model işlənilmişdir;

➢ Kompüter şəbəkələrində anomaliyaların aşkarlanması üçün maşın təlimi əsasında model işlənilmişdir;

➢ Kompüter şəbəkələrində zərərli proqramların aşkarlanması üçün dərin təlim əsasında model işlənilmişdir.

Praktik nöqteyi-nəzərdən işin nəticələri kibertəhlükəsizlik üzrə şəxslər, siyasətçilər və təşkilat rəhbərləri üçün mühüm əhəmiyyət kəsb edir. İşdə alınmış nəticələr kompüter şəbəkələrinin kiberdayanıqlığını artırmağa, həssas məlumatları və kritik aktivləri kibertəhlükələrdən qorumağa imkan verir.

Müdafiə üçün təqdim edilən vəzifələr:

➢ Kompüter şəbəkələrinin kibertəhlükəsizliyi və monitorinq texnologiyalarının analizi;

➢ Süni intellektin əsas üsulları və onların kibertəhlükəsizlikdə tətbiqi məsələlərinin analizi;

➢ Kompüter şəbəkələrində müdaxilələrin dərin təlim əsasında aşkarlanması modeli;

➢ Kompüter şəbəkələrində anomaliyaların maşın təlimi əsasında aşkarlanması modeli;

➢ Kompüter şəbəkələrində zərərli proqramların dərin təlim əsasında aşkarlanması modeli.

Dissertasiya işinin strukturu və həcmi. Dissertasiya işi giriş, 3 fəsil, nəticə və 42 ədəbiyyat siyahısından ibarətdir, 102 səhifədə şərh olunmuşdur. İşdə 36 şəkil və 4 cədvəl yer almışdır.

Dissertasiyada qrup üzvlərinin töhfələri.

Magistrantın adı	**Gördüyü işlər**
Aytən Hüseynova	Giriş, 1.1 Kompüter şəbəkələrinin kibertəhlükəsizliyinə təhdidlər 1.2 Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinin ənənəvi vasitələri, 2.3 Dərin təlim üsullarının analizi 3.1 Kompüter şəbəkələrinə müdaxilələrin dərin təlim əsasında aşkarlanması
Elnur İbrahimov	Giriş, 1.1 Kompüter şəbəkələrinin kibertəhlükəsizliyinə təhdidlər 1.2 Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinin ənənəvi vasitələri 1.4 Tədqiqat məsələlərinin qoyuluşu 2.3 Dərin təlim üsullarının analizi 3.1 Kompüter şəbəkələrinə müdaxilələrin dərin təlim əsasında aşkarlanması
Qiyas Cəfərov	Giriş,

	1.3 Kompüter şəbəkələrinin kibertəhlükəsizliyində süni intellekt texnologiyalarının rolu 2.1 Maşın təlimi və dərin təlim 2.2 Maşın təlimi üsullarının analizi 3.3 Kompüter şəbəkələrində zərərli proqramların dərin təlim əsasında aşkarlanması
Səməd Cabbarlı	Giriş, 1.3 Kompüter şəbəkələrinin kibertəhlükəsizliyində süni intellekt texnologiyalarının rolu 2.1 Maşın təlimi və dərin təlim 3.2 Kompüter şəbəkələrində anomaliyaların maşın təlimi əsasında aşkarlanması
Vüqar Stanbullu	Giriş, 1.4 Tədqiqat məsələlərinin qoyuluşu 2.2 Maşın təlimi üsullarının analizi 3.2 Kompüter şəbəkələrində anomaliyaların maşın təlimi əsasında aşkarlanması 3.3 Kompüter şəbəkələrində zərərli proqramların dərin təlim əsasında aşkarlanması

Minnətdarlıq. Müəlliflər tədqiqat işinin ərsəyə gəlməsində hərtərəfli dəstəyə, magistraturada təhsil aldığı müddətdə onlara göstərilən yüksək diqqət və qayğıya görə Azərbaycan Texniki Universitetinin “Kibertəhlükəsizlik” kafedrasının rəhbərliyinə, kafedranın bütün əməkdaşlarına və elmi rəhbər, texnika üzrə fəlsəfə doktoru, dosent Ramiz Şıxəliyevə dərin minnətdarlıqlarını bildirirlər.

I FƏSİL. KOMPÜTER ŞƏBƏKƏLƏRİNİN KİBERTƏHLÜKƏSİZLİYİ VƏ SÜNİ İNTELLEKT TEXNOLOGİYALARI

1.1. Kompüter şəbəkələrinin kibertəhlükəsizliyinə təhdidlər

Kompüter şəbəkələri daim müxtəlif təhdidlərə məruz qalır. Bu təhdidlər həm xarici, həm də daxili mənbələrdən gələ bilər. Kompüter şəbəkələrinin kibertəhlükəsizliyinə təhdidlər məlumat və resursların məxfiliyini, bütövlüyünü və ya əlçatanlığını pozmaq məqsədi ilə şəxslər, qruplar və ya avtomatlaşdırılmış sistemlər tərəfindən həyata keçirilən geniş spektrli zərərli fəaliyyətləri əhatə edir.

1.1.1 Kibertəhlükələrin növləri

Kompüter şəbəkələrinin kibertəhlükəsizliyinə olan təhdidlərə qarşı mübarizə texniki nəzarət, istifadəçilərin məlumatlandırması və təlimi, güclü təhlükəsizlik siyasəti və prosedurları, təhlükələrin intellektual analizini və s. tələb edir. Kompüter şəbəkələrinin kibertəhlükəsizliyinə olan bəzi təhdidləri analiz edək. Bu təhdidlərə aşağıdakılar aiddir:

- Zərərli proqram təminatı hücumları;
- Parol hücumları;
- Xidmətdən imtina hücumları;
- İnsayder hücumları;
- Sosial mühəndislik hücumları;
- Ortada adam hücumları (Man-in-the-Middle- MITM);
- Kod inyeksiyası hücumları.

Zərərli proqramlar

Kompüter sistemlərinə icazəsiz girişi pozmaq, idarə etmək və ya məxfi məlumatları əldə etmək üçün nəzərdə tutulmuş proqramdır. Zərərli proqramlara viruslar, şəbəkə soxulcanları, troyanlar, ransomware, casus proqramları və reklam proqramları daxildir. Zərərli proqramlar sistemləri e-poçt qoşmaları, proqram

yükləmələri, zərərli veb-saytlar və ya çıxarıla bilən media vasitəsilə yoluxdura bilər (Hansman, S., and Hunt, R., 2005).

Zərərli proqram hücumlarının növləri:

- Troyan: Qanuni proqram təminatı kimi maskalanaraq, zərərli giriş üçün arxa qapılar yaradırlar.
- Fidyə proqramı: Fidyə ödənilənə qədər istifadəçiləri sistemlərindən və ya məlumatlarından bloklayır.
- Vorm: Zəifliklərdən istifadə etmək üçün yayılan, özünü təkrarlayan zərərli proqram.
- Casus proqramı: İstifadəçi fəaliyyətini gizli şəkildə müşahidə edir və şəxsi məlumatları toplayır.
- Reklam proqramı: Reklam proqramı tez-tez pulsuz proqram təminatı ilə birləşir və arzuolunmaz reklamları göstərir.

Parol hücumları

Etibarlı istifadəçi adları və parolları təxmin etmək və ya əldə etmək yolu ilə bədniyyətlər tərəfindən sistemlərə, hesablara və ya məlumatlara icazəsiz giriş əldə etmək cəhdləridir. Bu hücumlar parol təhlükəsizliyi sistemlərinin zəifliklərdən istifadə edir və icazəsiz girişə, məlumatların pozulmasına və müxtəlif təhlükəsizlik insidentlərinə səbəb ola bilər.

Parol hücumlarının növləri:

- Kredensial doldurma (Credential Stuffing): Birdən çox saytda oğurlanmış hesab etimadnaməsini istifadə etmək.
- Parolun yayılması (Password spraying) İcazəsiz giriş əldə etmək üçün bir çox hesaba qarşı ümumi parollardan istifadə.
- Kobud Güc Hücumları (Brute Force attack): Düzgün parol tapılana qədər sistematik olaraq parolların təxmin edilməsi.

Xidmətdən imtina hücumları

Şəbəkənin, serverin və ya veb-saytın normal fəaliyyətini pozmaq məqsədi daşıyır və onu qanuni istifadəçilər üçün əlçatmaz edir.

Xidmətdən imtina hücumlarının növləri:

- Xidmətdən imtina (Denial of Service - DoS) hücumları xidməti pozmaq üçün sorğularla sistemi həddən artıq yükləyir.
- Paylanmış xidmətdən imtina (Distributed Denial of Service - DDoS) hücumları DoS hücumları kimidir, lakin xidməti pozmaq üçün bir çox mənbədən istifadə edir.

İnsayder hücumu

Təşkilat daxilindəki şəxslərin təşkilata qarşı zərərli fəaliyyətlərdə iştirak etməsidir. Bu hücumlar məlumat sızdırılması, sənaye casusluğu və sistemlərin sabotajı kimi formalarda ola bilər. Əsas səbəbləri arasında məmnuniyyətsizlik, maliyyə çətinlikləri və şəxsi mənfəət dayanır.İnsayder hücumlarının əsas xüsusiyyəti, hücum edən şəxsin təşkilat daxilində müəyyən bir səviyyədə etimada və giriş icazələrinə malik olmasıdır.

İnsayder hücumlarının bir neçə növü ola bilər:

- Məlumat sızdırılması (Data Leakage): İşçi və ya başqa bir şəxs məxfi məlumatları icazəsiz olaraq kənara çıxara bilər.
- Sənaye casusluğu (Industrial Espionage): Təşkilatın ticarət sirlərini və ya digər kritik məlumatlarını rəqiblərə və ya digər maraqlı tərəflərə ötürmək.
- Sistemlərə zərər vermək (Sabotage): Sistemləri, serverləri və ya digər kritik infrastrukturu qəsdən zədələmək.
- Fırıldaqçılıq (Fraud): Maliyyə mənfəəti üçün təşkilat daxilində saxta fəaliyyətlər həyata keçirmək.

İnsayder hücumlarının əsas səbəbləri arasında məmnuniyyətsizlik, maliyyə çətinlikləri, rəqabət, ideoloji səbəblər və ya şəxsi mənfəət dayanır. Bu hücumlar təşkilatlar üçün böyük təhlükə yaradır, çünki hücum edən şəxs daxili sistemlərə giriş icazəsinə malik olduğu üçün kənar hücumlardan daha çox təsirli ola bilər.

Sosial mühəndislik hücumları

Məxfi məlumatları yaymaq və ya təhlükəsizliyi pozan hərəkətlər etmək üçün manipulyasiya edir. Nümunələrə bəhanəçilik, yemləmə, arxadan qaçma və fişinq daxildir.

Sosial mühəndislik hücumlarının növləri:

- Fişinq: Həssas məlumatları oğurlamaq üçün aldadıcı ünsiyyətdir.
- Yayılan Fişinq (Spread Fishing): Xüsusi şəxslərə və ya təşkilatlara qarşı hədəflənmiş fişinqdir.
- Vişinq: Telefon zəngləri vasitəsilə olan fişinqdir.
- Smişinq: SMS mesajları vasitəsilə olan fişinqdir.

Ortada adam hücumları (Man-in-the-middle attack - MITM)

Təcavüzkarın bir-biri ilə birbaşa əlaqə saxladığına inanan iki tərəf arasındakı əlaqəni gizli şəkildə kəsdiyi və ya dəyişdirdiyi kiberhücumdır. Bu cür hücumlar məxfi məlumatların oğurlanmasına və ya zərərli kodun yeridilməsinə səbəb ola bilər.

Ortada adam hücumlarının növləri:

- Dinləmə (Eavesdropping): Məlumatları oğurlamaq üçün iki tərəf arasındakı əlaqəni kəsir.
- Sessiyanın yönəldilməsi (Session Hijacking): İdentifikasiyadan sonra istifadəçi sessiyasına nəzarət edir.

Kod inyeksiyası hücumları

Zərərli kodu sayta və məlumata bazasına daxil edərək icra olunan təhdid növüdür.

Kod inyeksiyası hücumlarının növləri:

- SQL inyeksiyası hücumları zərərli SQL kodunu giriş sahələrinə daxil etməklə SQL verilənlər bazalarından istifadə edən veb proqramları hədəf alır. Uğurlu hücum verilənlər bazalarına icazəsiz giriş, məlumatların oğurlanması və ya məlumatların manipulyasiyası ilə nəticələnə bilər.

- Saytlararası skriptləmə (Cross-Site Scripting) başqaları tərəfindən baxılan veb səhifələrə skriptlər daxil edir (J. Meira, R. Andrade, I. Praça, J. Carneiro, V. Bolón-Canedo, A. Alonso-Betanzos, and G. Marreiros, 2020).

1.2 Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqinin ənənəvi vasitələri

Kibertəhlükəsizlik monitorinqi konsepsiyası kompüter şəbəkələrində kibertəhlükəsizlik təhdidlərinin və zəifliklərinin tanınması, qiymətləndirilməsi və aradan qaldırılmasından ibarətdir. Kompüter şəbəkələrinin kibertəhlükəsizliyinin monitorinqi üçün müxtəlif ənənəvi vasitələrdən istifadə olunur.

Təhlükəsizlik məlumatı və hadisələrin idarə edilməsi (SIEM): SIEM sistemləri kibertəhlükəsizlik insidentlərini müəyyən etmək və onlara cavab vermək üçün loglar, şəbəkə trafiki, proqramlar və təhlükəsizlik cihazları daxil olmaqla məlumatları birləşdirir və əlaqələndirir. Təşkilatın informasiya təhlükəsizliyinin real vaxt rejimində görünüşünü təmin edir. Müxtəlif mənbələrdən daxilolma məlumatlarını toplayır və təhlil edir, təhlükəsizlik insidentlərini aşkar edir və xəbərdarlıqlar verir. ***SIEM sistemləri aşağıdakı funksiyaları həyata keçirir (Laura Wilson, 2019):***

- Şəbəkələrarası ekran, antivirus sistemləri, müdaxilənin aşkarlanması sistemləri, serverlər və proqramlar kimi müxtəlif mənbələrdən loq məlumatlarını toplayır, saxlayır və normallaşdırır.
- Müxtəlif mənbələrdən gələn hadisələri əlaqələndirir.
- Davamlı olaraq şübhəli fəaliyyətləri aşkar etmək üçün ətraf mühiti real vaxt rejimində monitorinq edir və potensial təhlükələr aşkar edildikdə siqnallar verir.
- Təhlükəsizlik insidentlərinin tədqiqatı, təhlili və aradan qaldırılması üçün alətlər təqdim etməklə insidentlərə cavab reaksiyanı asanlaşdırır.
- Audit və təhlükəsizlik nəzarəti əsasında daxili hesabat imkanları təqdim edir.

Müdaxilələrin aşkarlanması sistemi (IDS): İcazəsiz girişi, sui-istifadəni və ya kompüter şəbəkələrində pozuntuları aşkar etmək üçün nəzərdə tutulmuş şəbəkə təhlükəsizliyinin mühüm komponentidir. Şəbəkə resurslarına və kompüter şəbəkələrinə icazəsiz girişi aşkar edir. Müdaxilə aşkar edildikdən sonra sistem təhlükəsizlik işçilərini potensial təhdid barədə xəbərdar edir.

Müdaxilələrin aşkarlanması sisteminin növləri:

- Şəbəkəyə əsaslanan müdaxilənin aşkarlanması sistemləri (NIDS) şübhəli fəaliyyət axtararaq təşkilatın şəbəkəsində trafikə nəzarət edir. Şəbəkədəki trafikə nəzarət etmək üçün strateji nöqtələrə yerləşdirilir. O, şəbəkələrarası ekranların aşkar edə bilmədiyi zərərli paketləri aşkar edə bilər.
- Host əsaslı müdaxilənin aşkarlanması sistemləri (HIDS) fərdi cihazlarda və ya hostlarda işləyir, yalnız cihazdan gələn və gedən paketləri izləyir və şübhəli fəaliyyət barədə xəbərdarlıq edir. Proqram qeydlərini, fayl sisteminin modifikasiyalarını təhlil edərək baş verənlər haqqında məlumat verir (J. Veeramreddy and K. Prasad, 2019).

Aşkarlama üsulları:

- Siqnatura əsaslı aşkarlama: Potensial təhlükəni göstərən məlum təhlükə siqnaturaları və ya məlumat nümunələrinə əsaslanır.
- Anomaliyaya əsaslanan aşkarlama şəbəkə trafikinə nəzarət edir və onu şəbəkə davranışının müəyyən edilmiş bazası ilə müqayisə edir. Bu zaman hər hansı anomalik davranış şübhəli kimi qeyd olunur. Bu üsul potensial olaraq yeni hücumları müəyyən edir, lakin siqnatura əsaslı aşkarlama ilə müqayisədə daha çox yanlış pozitivlər yarada bilər.
- Stasionar protokol təhlili müşahidə edilən hadisələri ümumi qəbul edilmiş normal fəaliyyət profilləri ilə müqayisə edərək kənarlaşmaları müəyyən edir.

Müdaxilələrin qarşısının alınması sistemi (IPS): Şəbəkə və sistem trafikini zərərli fəaliyyətlərə və ya təhlükəsizlik siyasətinin pozulmasına görə yoxlayan şəbəkə təhlükəsizliyi texnologiyasıdır. İnsan müdaxiləsi olmadan aşkar edilmiş təhlükələri

avtomatik bloklamaq və ya qarşısını almaq qabiliyyətinə malikdir (Yin C, Zhu Y, Fei J, He X, 2017). Sistem tərəfindən real vaxt rejimində müəyyən edilən hücumların dayandırılması, xəta törədən IP ünvanının və ya trafikin bloklanması kimi funksiyaları icra edir. Təhlükənin aşkarlanması və azaldılması prosesini avtomatlaşdırır, əl ilə müdaxilə ehtiyacını azaldır və cavab vaxtlarını sürətləndirir.

Şəbəkələrarası ekran (Firewall): Təşkilatın əvvəllər müəyyən edilmiş təhlükəsizlik siyasətləri əsasında daxil olan və gedən şəbəkə trafikini izləyən və filtrləyən şəbəkə təhlükəsizlik vasitəsidir. Şəbəkələrarası ekranlarının əsas məqsədi zərərli trafikin şəbəkəyə daxil olmasının qarşısını almaq və məlumat sızması riskini minimuma endirmək üçün gedən trafik axınına nəzarət etməkdir. Etibarlı daxili şəbəkə ilə etibarsız xarici şəbəkələr arasında maneə yaradaraq şəbəkədaxili icazəsiz girişin qarşısının alınmasında iştirak edir.

Şəbəkələrarası ekranların növləri:

- Paket filtrləmə şəbəkələrarası ekranı: Paketləri yoxlayan və əvvəlcədən müəyyən edilmiş qaydalar əsasında onlara icazə verən və ya bloklayan təhlükəsizlik divarı növüdür. O, məzmununu yoxlamaq üçün paketi açmadan mənbə və təyinat IP ünvanlarına, port nömrələrinə və digər məlumatlara baxır.
- Veb tətbiq şəbəkələrarası ekranı (WAF): Xüsusilə veb proqramları qorumaq üçün nəzərdə tutulur və HTTP/HTTPS paketlərinin məzmununu yoxlayır. Onlar veb proqramlar üçün ümumi təhdidlər olan saytlar arası skript və SQL inyeksiyası kimi hücumların qarşısını almaq üçün istifadə olunur.
- Bulud şəbəkələrarası ekranı: Buludda yerləşdirilir və bulud xidməti kimi şəbəkə təhlükəsizliyini təmin edir. Miqyaslana bilən, sərfəli və virtuallaşdırılmış infrastrukturları, o cümlədən çox buludlu mühitləri qorumaq üçün idealdır.
- Proksi şəbəkələrarası ekranı: O, daxili şəbəkə və trafik mənbəyi arasında olan trafiki süzmək üçün proqram səviyyəsində işləyir. Digər serverlərdən resurslar axtaran müştərilərin sorğuları üçün vasitəçi kimi çıxış edir, trafiki

yönləndirməzdən əvvəl təhlükəsizlik qaydalarını tətbiq etmək üçün bütün paketi və məzmununu yoxlayır (Laura Wilson, 2019).

Əsas Xüsusiyyətləri:

- Girişə nəzarət edir.
- Trafiki yoxlayır.
- Virtual Şəxsi Şəbəkə (VPN) dəstəyi mövcuddur.
- Trafik haqqında ətraflı qeydlər və hesabatlar təqdim edir

Loq idarəetmə: Sistem və tətbiqetmə qeydlərini toplamaq, saxlamaq, təhlil etmək və hesabat vermək üçün istifadə olunur. Bu sistemlər həmçinin təhlükəsizlik hadisələrini aşkar etmək, araşdırmaq və reaksiya vermək üçün də vacibdir.

Əsas Funksiyaları:

- Müxtəlif mənbələrdən loq məlumatlarını toplamaq
- Məlumatları birləşdirilmiş və oxunaqlı bir formatda təqdim etmək
- Məlumatları mərkəzləşdirilmiş bir anbarda saxlamaq
- Məlumatları təhlil etmək
- Təhlil nəticələrinə əsasən hesabatlar hazırlamaq

Son nöqtənin aşkarlanması və cavablandırılması (EDR):

Son nöqtələrdə təhlükəsizlik təhdidlərini aşkar etmək, araşdırmaq və onlara cavab vermək üçün istifadə edilən mütərəqqi təhlükəsizlik texnologiyalarını ifadə edir. Notbuklarda, masaüstü kompüterlərdə və mobil cihazlarda zərərli proqramların və digər təhlükələrin müəyyən edilməsində iştirak edir (Faitouri A. Aboaoja, Anazida Zainal,Fuad A. Ghaleb,Bander Ali Saleh Al-rimy,Taiseer Abdalla Elfadil Eisa andAsma Abbas Hassan Elnour, 2022).

Əsas Funksiyaları:

- Forensik tədqiqatlar aparmaq
- Təhlükəsizlik hadisələrini araşdırmaq

- Şübhəli və ya zərərli davranışları aşkar etmək
- Təhlükəli faylları silmək və şübhəli əlaqələri kəsmək

Zəiflik skaneri:

Təşkilatların şəbəkələrində, sistemlərində və tətbiqlərində zəiflikləri aşkar etmək və qiymətləndirmək üçün istifadə olunan bir təhlükəsizlik vasitəsidir. Bu skanerlər, məlumatların müdafiəsini gücləndirmək və potensial təhdidlərə qarşı müqaviməti artırmaq məqsədilə zəif nöqtələri müəyyən edir və onları təhlil edir (Anderson, J. P., 1980).

Əsas Funksiyaları:

- Zəifliklərin aşkarlanması
- Aşkarlanan zəifliklərin təsir dərəcəsini müəyyən etmək.
- Zəifliklər haqqında ətraflı hesabatlar təqdim etmək
- Daimi monitorinq və təkrar skan etmək

Antivirus: Kompüter şəbəkələrində zərərli proqramlarını aşkar etmək, qarşısını almaq və aradan qaldırmaq üçün nəzərdə tutulmuş proqram növüdür. Bu proqramlar məlum zərərli proqramlara uyğun gələn nümunələr və ya siqnaturalar üçün kompüterdəki faylları və proqramları skan etməklə işləyir. O, həmçinin zərərli proqramın mövcudluğunu göstərə bilən şübhəli davranışı və ya kodu müəyyən etmək üçün evristik analizdən istifadə edə bilər. Zərərli proqram aşkar edildikdən sonra antivirus proqramı zərərli faylları karantinə qoya, silə və ya onların vurduğu zərəri bərpa etməyə cəhd edə bilər (Anderson, J. P., 1980).

Antivirus proqramının əsas xüsusiyyətləri:

- Real vaxt rejimində qoruma
- Planlaşdırılmış skanlar
- Avtomatik yeniləmələr
- Karantinə almaq

Antivirus proqramlarının növləri:

- Ənənəvi antivirus: Siqnatura əsaslı aşkarlamaya əsaslanan klassik antivirus proqramlarıdır.
- Növbəti nəsil antivirus (NGAV): Maşın təlimi, davranış analizi və süni intellekt kimi qabaqcıl metodları özündə birləşdirərək ənənəvi metodlardan kənara çıxır.
- Bulud əsaslı antivirus: Bu həllər yeni təhdidləri daha tez aşkar etməyə imkan verən real vaxt rejimində faylların skan edilməsi və təhlili üçün bulud resurslarından istifadə edir (Ramin Abbasov, 2017).

Şəbəkə trafikinin analizi (NTA): Şəbəkə trafiqinin dərin analizini həyata keçirərək hər hansı şübhəli fəaliyyətləri aşkar etmək üçün istifadə olunur. Real vaxt rejimində çalışaraq, şəbəkə məlumatlarını toplayır, təhlil edir və hər cür potensial təhdidlərə qarşı xəbərdarlıq verir.

Əsas Funksiyaları:

- Trafikin real vaxt rejimində izləyərək anormal davranışları aşkar etmək
- Potensial təhdidlər haqqında dərhal xəbərdarlıq vermək
- Təhdidin mənbəyini və onun şəbəkəyə necə təsir etdiyini dərindən araşdırmaq
- İstifadəçi və cihaz fəaliyyətlərini normadan kənar davranışları aşkar etmək

Təhlükəsizlik Konfiqurasiyasının Qiymətləndirilməsi (SCA): Təşkilatın təhlükəsizlik konfiqurasiyasının vəziyyətini qiymətləndirən bir prosesdir. Bu, təşkilatın təhlükəsizlik siyasətlərinə və standartlara uyğun olaraq sistemlərinin düzgün konfiqurasiya edilib-edilmədiyini yoxlayır. Zəiflikləri azaltmaq və normativlərə uyğunluğu qorumaq üçün təhlükəsizlik konfiqurasiyası prosesinin avtomatlaşdırılması rolunu oynayır (Sevinc Nərimanova, 2021).

Əsas Funksiyaları:

- Sistem və şəbəkə konfiqurasiyalarının standartlara uyğunluğunu təmin etmək.
- Potensial zəifliklər olan konfiqurasiya parametrlərini müəyyən etmək.

- Təhlükəsizlik siyasətinə uyğun tədbirlərin həyata keçirilməsini təmin etmək.

1.3. Kompüter şəbəkələrinin kibertəhlükəsizliyində süni intellekt texnologiyalarının rolu

Kompüter şəbəkələrinin kibertəhlükəsizliyi müasir rəqəmsal infrastrukturun mühüm aspektidir və şəbəkələri icazəsiz girişdən, məlumatların pozulmasından və kiberhücumlardan qorumağa yönəlmiş geniş tədbirlər və təcrübələri əhatə edir. Qurğuların və sistemlərin artan qarşılıqlı əlaqəsi ilə kompüter şəbəkələrinin təhlükəsizliyinin təmin edilməsi həssas məlumatların qorunması, əməliyyat davamlılığının təmin edilməsi və istifadəçilərin etibarının qorunması üçün mühüm əhəmiyyət kəsb edir.

Kompüter şəbəkələrinin kibertəhlükəsizliyi üçün əsas problemlərdən biri hücumların tez-tez görünüşünü və vektorlarını dəyişdirməsidir. Yeni növ hücum və ya zərərli proqram hücumu zamanı ənənəvi sistem tərəfindən bu davranışları aşkar etmək və müəyyən etmək mümkün deyil, çünki onların uyğunlaşdırıla biləcəyi sabit qaydalar və ya əvvəlki nümunələr yoxdur. Bu vəziyyətin tipik nümunəsi sıfır gün hücumlarıdır.

Şəbəkə kibertəhlükəsizliyinin əsas komponentlərindən biri şəbəkəyə daxil olan və çıxan trafiki tənzimləmək üçün firewall-ların, müdaxilənin aşkarlanması və qarşısının alınması sistemlərinin və girişə nəzarətin tətbiqini əhatə edən mühafizə sistemidir. Bu mexanizmlər zərərli trafiki süzərək şəbəkə resurslarına icazəsiz girişin qarşısını alaraq xarici təhlükələrə qarşı ilk müdafiə xətti rolunu oynayır (Sevinc Nərimanova, 2021).

Şəbəkə məlumatlarının şifrələməsi ötürülən məlumatların təhlükəsizliyində mühüm rol oynayır və həssas məlumatların şəbəkələr arasında ötürülməsi zamanı məxfi qalmasını və müdaxiləyə qarşı davamlı olmasını təmin edir (Tural Quliyev, 2020). İSO OSI modelinin nəqliyyat səviyyəsində təhlükəsizliyinin təmin edilməsi və virtual xüsusi şəbəkələrin istifadəsi təhlükəsiz əlaqə kanalları yaratmaq və məlumatların pis niyyətli şəxslər tərəfindən dinlənilməsi və ya ələ keçirilməsindən qorunmağa imkan verir.

Şəbəkə seqmentasiyası potensial pozuntuları ehtiva etmək və zərərli proqramların və ya icazəsiz fəaliyyətlərin yayılmasını məhdudlaşdırmaq üçün böyük şəbəkələri daha kiçik, təcrid olunmuş seqmentlərə bölməkdir. Hər bir seqmentdə girişə nəzarət və təhlükəsizlik siyasətini tətbiq etməklə, təşkilatlar təhlükəsizlik insidentlərinin təsirini effektiv şəkildə azalda və şəbəkə daxilində təcavüzkarların hərəkətinin qarşısını ala bilər.

Davamlı monitorinq və təhlükənin aşkarlanması real vaxt rejimində təhlükəsizlik insidentlərini müəyyən etmək və onlara cavab vermək üçün vacibdir. Müdaxilənin aşkarlanması sistemləri, təhlükəsizlik məlumatı və hadisə idarəetmə platformaları kimi şəbəkə təhlükəsizliyi monitorinqi alətləri şəbəkə trafikinin nümunələrini təhlil edir, şübhəli davranışı aşkar edir və operativ araşdırma və aradan qaldırılması üçün xəbərdarlıqlar yaradır.

Müntəzəm təhlükəsizlik monitorinqi, zəifliyin qiymətləndirilməsi və nüfuz testi şəbəkə təhlükəsizliyi tədbirlərinin effektivliyini qiymətləndirmək və müdafiə sistemlərində potensial zəiflikləri və ya boşluqları müəyyən etmək üçün zəruridir (Sevinc Nərimanova, 2021).

Kompüter şəbəkələrinin kibertəhlükəsizliyinin effektiv şəkildə təmin edilməsi texniki nəzarəti, şifrələmə protokollarını, seqmentləşdirmə strategiyalarını, monitorinq alətlərini və proaktiv təhlükəsizlik təcrübələrini birləşdirən çoxşaxəli yanaşma tələb edir (Sevinc Nərimanova, 2021). Güclü şəbəkə təhlükəsizliyi tədbirləri həyata keçirməklə təşkilatlar öz şəbəkələrini gücləndirə və kiberhücum riskini azalda, bununla da kritik aktivləri qoruya və rəqəmsal resursların bütövlüyünü və əlçatanlığını təmin edə bilərlər.

Süni intellekt (Sİ) maşınların insan intellektini imitasiya etdiyi və həmin zəkanın maşın görmə, ekspert sistemləri, təbii dilin emalı və nitqin tanınması və bir çox digər tətbiqlərdə tətbiq olunduğu texnoloji prosesdir. Süni intellekt sürətlə inkişaf etdi və bir çox sahələrə və hətta gündəlik həyatımıza daxil oldu. Bununla belə, Sİ-nin kiberfiziki sahəyə daxil olması, istər hücumda, istərsə də müdafiədə kibertəhlükəsizliyin simasını həmişəlik dəyişdi.

Bu gün müəssisələr və fərdlər üçün internetdən asılılıq səbəbindən biznes və fiziki şəxslərin hər hansı formada kiberhücumlardan qorunmağa ehtiyacı var. Kibertəhlükəsizlik bu cür hücumların dayandırıla və ya aradan qaldırıla biləcəyi texnoloji təcrübədir. Kibertəhlükəsizlik olduqca genişlənən bir sahədir və "Statista" statistik məlumat mərkəzinin məlumatlarına görə kibertəhlükəsizlik bazarının 2024-cü ildə təxminən 14,30 milyard dollar olacağı proqnozlaşdırılır.

Kibertəhlükəsizlikdə Sİ-nin istifadəsi çoxşaxəlidir. O, təhdidləri dərk etmək və onları əvvəlcədən dayandırmaq, həmçinin mümkün pozuntu ilə bağlı riskləri aradan qaldırmaq üçün istifadə edilə bilər (Tural Quliyev, 2020). Məsələn, MT alqoritmləri kompüter şəbəkələrinin kibertəhlükəsizliyinin təmin edilməsi ilə bağlı müxtəlif məsələləri həll etmək üçün istifadə edilə bilər

Süni intellekt kompüter şəbəkələrinin monitorinqi, idarə edilməsi və optimallaşdırılması məsələlərində istifadəsi yeni bir mərhələ açdı və şəbəkə trafikinin analizi sahəsində evvektiv texnologiya kimi ortaya çıxdı. Qabaqcıl alqoritmlərdən, MT modellərindən və real vaxt rejimində məlumatların emalı imkanlarından istifadə etməklə şəbəkə trafiknin analizi sistemləri yaradıldı. Şəbəkə trafikini analizində Sİ-nin əsas tətbiqlərindən biri trafik proqnozlaşdırılmasıdır ki, burada MT alqoritmləri gələcək trafik nümunələrini yüksək dəqiqliklə proqnozlaşdırmaq üçün tarixi trafik məlumatlarını analiz edir. Bu proqnozlar şəbəkə trafikinin effektiv idarə edilməsini, şəbəkə ötürmə kanallarının səmərəli istifadə edilməsini və kompüter şəbəkələrinin kibertəhlükəsizliyinin təmin edilməsinə imkan verir.

Bununla belə, şəbəkə trafikin analizində Sİ-nin geniş tətbiqi bir sıra problemlər yaradır. Həssas məlumatlarının məxfiliyinin və təhlükəsizliyinin təmin edilməsi mühüm əhəmiyyət kəsb etdiyi üçün, icazəsiz giriş və məlumatların pozulmasından qorunmaq üçün etibarlı məlumat anonimləşdirmə üsulları, şifrələmə protokolları və giriş nəzarətləri tələb edir.

Anomaliyaların, virusların və zərərli proqramların aşkarlanması da kibertəhlükəsizliyin təmin edilməsinin kritik aspektidir və rəqəmsal aktivlərin qoruması, həssas məlumatın qoruması, kompüter sistemləri və şəbəkələrinin bütövlüyünü qoruması üçün vacibdir. Mürəkkəb kibertəhlükələrin yayılması və inkişaf

edən hücum üsullarının yaranması ilə anomaliyaların, virusların və zərərli proqramların aşkarlanması və azaldılması getdikcə çətinləşir və qabaqcıl aşkarlama metodları və texnologiyalarının tətbiqini tələb edir.

Anomaliyaların aşkarlanmasına əsas yanaşmalardan biri normal fəaliyyətdən kənarlaşmaları müəyyən etmək üçün şəbəkə trafikində, sistem qeydlərində və istifadəçi davranışında nümunələri analiz edən MT alqoritmlərinin istifadəsidir. Tarixi məlumatlar üzrə xüsusiyyətləri öyrətməklə klasterləşdirmə və təsnifat üsullardan istifadə etməklə, MT-nə əsaslanan anomaliya aşkarlama sistemləri əvvəllər görünməmiş təhdidləri və yaranan hücum nümunələrini effektiv şəkildə aşkarlaya bilər. Bu da təhlükənin proaktiv şəkildə azaldılması və cavablandırılmasına imkan verir.

Adətən siqnatura əsaslı aşkarlama metodlar məlum zərərli proqramların verilənlər bazasındakı fayl siqnaturalarının və ya davranış nümunələrini müqayisə etməklə məlum virusları və zərərli proqramları müəyyən etmək üçün istifadə olunur. Məlum təhlükələri aşkar etmək üçün effektiv olsa da, siqnatura əsaslı aşkarlama "sıfır günü" hücumları və siqnatura əsaslı aşkarlama mexanizmlərindən yayınan polimorfik zərərli proqram variantlarını aşkar etməkdə məhdudiyyətlərə malikdir. Bu problemi həll etmək üçün şübhəli və ya zərərli fəaliyyəti müəyyən etmək üçün fayl və ya proseslərin davranışını və xüsusiyyətlərini analiz edən evristik və davranışa əsaslanan aşkarlama üsullarından istifadə edilir. Evristik analiz əvvəlcədən müəyyən edilmiş qaydalar və ya alqoritmlər əsasında potensial zərərli kod nümunələri və ya davranışların müəyyən edilməsini nəzərdə tutur, davranışa əsaslanan analiz isə zərərli proqram fəaliyyətinin göstəricisi olan anomaliya davranış üçün proqramların və proseslərin icrasına nəzarət edir.

Avtomatlaşdırılmış aşkarlama metodlarına əlavə olaraq, anomaliyaların, virusların və zərərli proqramların aşkar edilməsində "əl ilə təhlil" və təhlükə kəşfiyyatı mühüm rol oynayır. Təhlükəsizlik analitikləri və insidentlərə cavab verən qruplar şübhəli faylları təhlil etmək, hücum vektorlarını müəyyən etmək və kiber təhdidləri xüsusi təhlükə faktorlarına və ya qruplaşmalarına aid etmək üçün təhdid kəşfiyyatı, zərərli proqram sandbox-larından və əks mühəndislik üsullarından istifadə edirlər.

Təhlükələrin aşkarlanmasına bu yanaşma təşkilatlara təhlükəsizlik xəbərdarlıqlarını kontekstləşdirməyə və prioritetləşdirməyə, təhlükəsizlik insidentlərinə effektiv reaksiya verməyə və müdafiə vasitələrini inkişaf edən təhdidlərə uyğunlaşdırmağa imkan verir (Vahid Cavadov, 2019).

Təhdidlərin aşkarlanması alətlərinin və təhlükəsizlik məlumatı və hadisələrin idarə edilməsi platformalarının inteqrasiyası müxtəlif İT mühitlərində təhlükəsizlik hadisələrinin və anomaliyalarının mərkəzləşdirilmiş monitorinqinə, korrelyasiyasına və analizinə imkan verir (Elvin Məmmədov, 2019). Təhdidlərin aşkarlanması alətlərinin və təhlükəsizlik məlumatı və hadisələrin idarə edilməsi həlləri şəbəkə avadanlıqları, son nöqtələr və təhlükəsizlik vasitələri da daxil olmaqla bir çox mənbədən olan məlumatları birləşdirir və əlaqələndirir və təhlükəsizlik qruplarına real vaxt rejimində təhlükəsizlik insidentlərini aşkar etməyə və onlara cavab verməyə imkan verir. Bundan əlavə, son nöqtənin aşkarlanması və cavablandırılması həllərinin istifadəsi təşkilatlara son nöqtə fəaliyyəti və davranışı haqqında məlumatla təmin edir və son nöqtə səviyyəsində zərərli proqramların və digər zərərli fəaliyyətlərin aşkar edilməsini və saxlanmasını asanlaşdırır.

Anomaliyaların aşkarlanması və təhlükənin azaldılması texnologiyalarında irəliləyişlərə baxmayaraq, anomaliyaların, virusların və zərərli proqramların aşkarlanması kibertəhlükələrin inkişaf edən təbiəti və mürəkkəb hücum üsullarının yayılması səbəbindən davamlı problem olaraq qalır. Təşkilatlar anomaliyaları, virusları və zərərli proqramları effektiv şəkildə aşkar etmək və azaltmaq üçün proaktiv təhdidlərin aşkarlanması, davamlı monitorinq və insidentlərə reaksiya imkanlarını birləşdirərək kibertəhlükəsizliyə ayrı-ayrılıqda yanaşma tətbiq etməlidir. Avtomatlaşdırılmış aşkarlama metodları, təhlükə kəşfiyyatı və insan təcrübəsindən istifadə etməklə təşkilatlar müdafiələrini gücləndirə, kiber riskləri azalda və kritik aktivləri yaranan kibertəhlükələrdən qoruna bilərlər (Vahid Cavadov, 2019).

Kiberhücumların proqnozlaşdırılması da digər proseslər kimi mürəkkəb və dinamik bir işdir və qabaqcıl təhlükə kəşfiyyatını, maşın təlim alqoritmlərini və proaktiv təhlükəsizlik tədbirlərini əhatə edən çoxşaxəli yanaşma tələb edir. Tarixi hücum nümunələrini, kəşfiyyat fəaliyyətlərini və kompromis göstəricilərini təhlil

edərək kibertəhlükəsizlik mütəxəssisləri gələcək kiberhücumları qabaqcadan göstərə biləcək tendensiyaları və yaranan təhlükələri müəyyən edə bilərlər. Bundan əlavə, nüfuzlu mənbələrdən təhdid kəşfiyyatı xəbərləri təhdid subyektləri tərəfindən tətbiq edilən taktika, texnika və prosedurlar haqqında dəyərli fikirlər təqdim edərək, təşkilatlara potensial hücum vektorlarını qabaqcadan görməyə və hazırlamağa imkan verir. MT alqoritmləri anomaliya davranışı aşkar etmək, zərərli fəaliyyəti göstərən nümunələri müəyyən etmək və potensial kibertəhlükələri onlar reallaşmamışdan əvvəl proqnozlaşdırmaq üçün böyük məlumat dəstləri və alqoritmik modellərdən istifadə edərək, proqnozlaşdırıcı analitikada mühüm rol oynayır. Bu alqoritmlər kompromislərin incə göstəricilərini və yaranan hücum tendensiyalarını aşkar etmək üçün şəbəkə trafiki, sistem qeydləri və istifadəçi davranışı da daxil olmaqla geniş spektrli məlumat mənbələrini analiz edir. Zəifliyin qiymətləndirilməsi, nüfuz sınağı və təhlükəsizlik monitorinqi kimi proaktiv təhlükəsizlik tədbirləri İT infrastrukturundakı zəiflikləri təcavüzkarlar tərəfindən istismar edilməzdən əvvəl müəyyən etməyə və aradan qaldırmağa kömək edir. Proqnozlaşdırma üsulları, insidentlərə cavab vermə hazırlığı və işçilərin təlimini birləşdirərək, təşkilatlar kiberhücumları proqnozlaşdırmaq, qarşısını almaq və yumşaltmaq bacarıqlarını artıra, bununla da məlumatların pozulması, maliyyə itkilərini və risklərini azalda bilər (Anderson, J. P., 1980).

1.4. Tədqiqat məsələlərinin qoyuluşu

Elmi tədqiqatların aparılmış sistemləşdirməsi və müqayisəli analizi nəticəsində bu dissertasiya işində aşağıdakı tədqiqat məsələləri qoyulmuşdur:

➢ Kompüter şəbəkələrinin kibertəhlükəsizliyi və mövcud monitorinq texnologiyalarının analizi.

➢ Süni intellektin əsas üsullarının və onların kibertəhlükəsizlikdə tətbiqinin analizi.

➢ Kompüter şəbəkələrində müdaxilələrin dərin təlim əsasında aşkarlanması modelinin işlənilməsi.

➢ Kompüter şəbəkələrində anomaliyaların maşın təlimi əsasında aşkarlanması modelinin işlənilməsi.

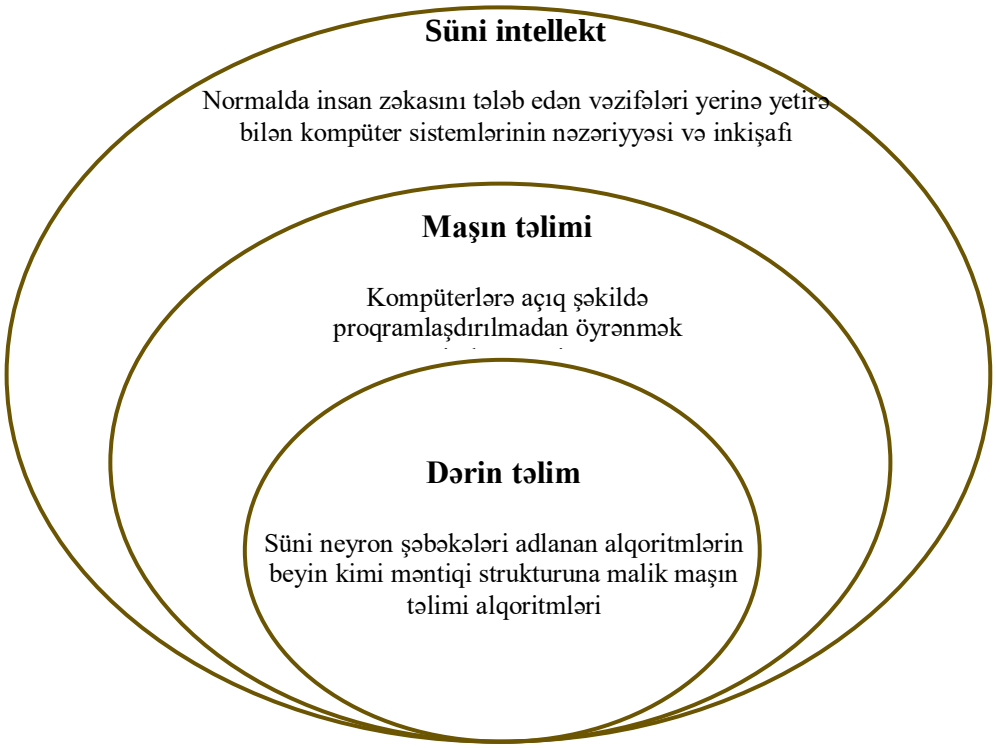
➢ Kompüter şəbəkələrində zərərli proqramların dərin təlim əsasında aşkarlanması modelinin işlənilməsi.

➢ İşlənmiş modellərin effektivliyinin və dəqiqliyinin qiymətləndirməsi üçün açıq verilənlər dəsti üzərində eksperimental tədqiqi.

II FƏSİL. MÖVCUD SÜNİ İNTELLEKT TEXNOLOGİYALARININ ANALİZİ

2.1. Maşın təlimi və dərin təlim

Süni intellekt texnologiyaları kompüter elminin bir sahəsidir. Süni neyron şəbəkələri süni intellektin sadələşdirilmiş bir modelidir və neyronlar insan beynində olduğu kimi digər neyronları aktivləşdirir. Dərin təlim və maşın təlimi süni intellekt texnologiyalarının əsas anlayışlarıdır. Süni intellekt texnologiyalarını daha yaxşı başa düşmək üçün bu anlayışları analiz edək (Şəkil 2.1). Sadə dillə desək, maşın təlimi, açıq şəkildə proqramlaşdırılmadan bir tapşırığı yerinə yetirməsi üçün alqoritmlərdən istifadə edərək məlumatlardan nəticə çıxararaq qərarlar qəbul edən kompüterlər deməkdir. Dərin təlim isə insan beynində modelləşdirilmiş alqoritmlərin mürəkkəb strukturundan istifadə edir. Bu, sənədlər, şəkillər və mətn kimi strukturlaşdırılmamış məlumatların emalına imkan verir.



Şək. 2.1. Süni intellekt texnologiyaları (Jennifer Martinez, 2018)

Maşın təlimi süni intellektin bir növüdür. Dərin təlim isə maşın təliminin xüsusilə mürəkkəb hissəsidir. Bunu bir cümlə ilə bu şəkildə ifadə etməyimiz düzgün

olar ki, dərin təlim, öz növbəsində, süni intellektin alt hissəsi olan maşın təliminin xüsusi alt kateqoriyasıdır (J. Cai, J. Luo, S. Wang, and S. Yang, 2018). Maşın təlimi alqoritmlərin açıq şəkildə proqramlaşdırılmadan konkret tapşırığı yerinə yetirmək üçün istifadə olunduğu kompüter elmi ilə statistikanın kəsişməsini təsvir edir və verilənlərdəki nümunələri tanıyır və yeni məlumatlar gəldikdən sonra proqnozlar verirlər. Ümumən, bu alqoritmlərin təlim prosesi alqoritmləri təmin etmək üçün istifadə olunan məlumatlardan asılı olaraq iki hissəyə bölünür:

1. Nəzarətli təlim.
2. Nəzarətsiz təlim.

Maşın təliminin hərəkətverici qüvvəsi adi statistikadır. Əvvəl də qeyd etdiyimiz üzrə, burada alqoritm açıq şəkildə proqramlaşdırılmadan, yalnız nümunələrə və nəticəyə əsaslanaraq proqnoz verməyi əsas tutur. Maşın təlimi alqoritmləri təlim məlumatlarına əsaslanan modellər qurur ki, bu da modellərə proqnozlar verməyə imkan verir (D. Michie, D. J. Spiegelhalter, and C. Taylor, 1994).

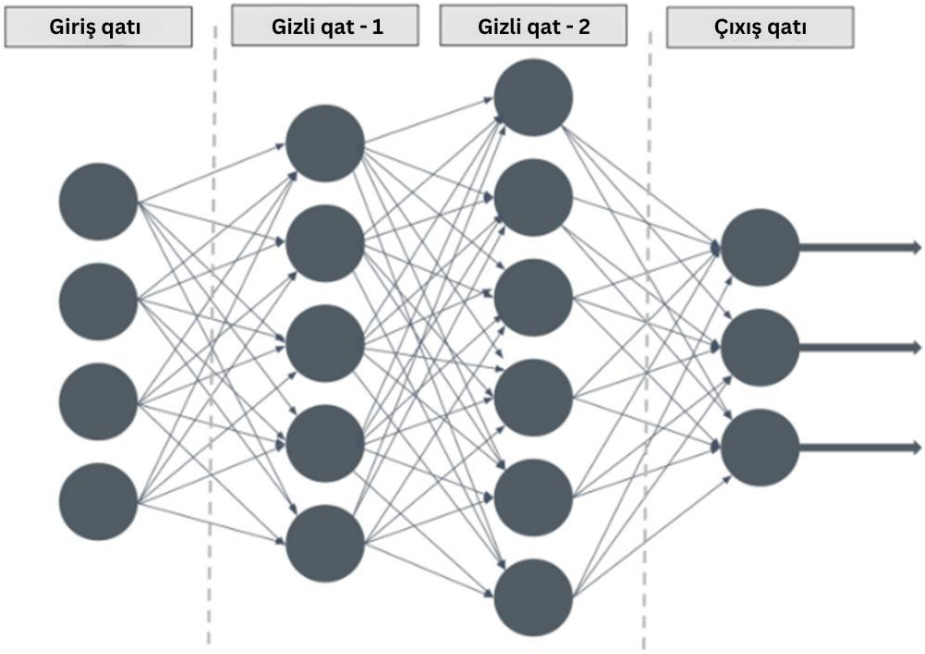
Maşın təlimi metodları kompüter şəbəkələrinin kibertəhlükəsizliyinin təmin edilməsi üçün avtomatlaşdırılmış və yeni hücumların erkən aşkarlanması və fişinq vebsaytlarının aşkarlanmasında tətbiq edilir (Kulkarni and L. L. Brown, 2019).

Dərin təlim alqoritmləri maşın təlimi alqoritmlərinin həm mürəkkəb bir forması kimi, həm də riyazi cəhətdən mürəkkəb dəyişikliyə məruz qalmış bir növü kimi qəbul edilə bilər. Bu sahəyə son zamanlar çox diqqət yetirilir, çünki, elmi tərəqqidə son inkişaf əvvəllər mümkün olmadığı düşünülən nəticələrə gətirib çıxardı. Dərin təlim, insanın nəticə çıxarmasına bənzər məntiqi strukturu ilə məlumatları analiz edən alqoritmləri təsvir edir. Bu proses də eynən maşın təlimindəki kimi, iki təlim yolu ilə baş tutur:

1. Nəzarətli təlim.
2. Nəzarətsiz təlim.

Buna nail olmaq üçün dərin təlim modelləri süni neyron şəbəkəsi adlanan çoxlaylı alqoritm strukturundan istifadə edir. Belə bir strukturun dizaynı insan beyninin bioloji neyron şəbəkəsindən ilhamlanıb və standart maşın təlimi modellərindən daha bacarıqlı təlim prosesinə gətirib çıxarır.

Şəkil 2.2-dəki nümunəni nəzərdən keçirərək sadə şəkildə deyə bilərik ki, gizli laylar şəbəkənin "həcmini və strukturunu" təyin etmək üçün istifadə etdiyi hesablanmış dəyərlərdir. Şəbəkənin giriş və çıxış layları arasında nə qədər çox gizli lay varsa, bir o qədər dərindir. Ümumiyyətlə, iki və ya daha çox gizli layı olan istənilən şəbəkə dərin neyron şəbəkəsi adlanır (Géron, A. , 2019).



Şək. 2.2. Süni neyron şəbəkəsi (Jennifer Martinez, 2018)

Bu gün dərin təlim bir çox sahələrdə istifadə olunur. Məsələn, özü özünü idarə edən və ya sürücüsüz nəqliyyat vasitələrində dərin təlim dayanma yol nişanlarını və ya piyadalar kimi obyektləri aşkar edilməsi, peyklər vasitəsi ilə obyektlərin aşkar edilməsi üçün və s. istifadə edilir. Həmçinin, kompüter sistemlərinin kibertəhlükəsizliyinin təmin edilməsi üçün dərin təlim modellərindən istifadə edilir və ədəbiyyatda bir çox tədqiqatlar var (Jennifer Martinez, 2018).

Ümumilikdə, avtomatlaşdırma və özünü təlim imkanları sayəsində dərin təlim alqoritmləri çox az miqdarda insan müdaxiləsinə ehtiyac duyur. Bu, dərin təlimin böyük potensialını göstərsə də, onun yaxın dövrümüzdə bu qədər istifadə edilməsinə duyulan ehtiyacın qarşılanması üçün iki əsas tələbi var (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018):

1. Məlumatların mövcudluğu.

2. Hesablamaların güclü olması.

Birinci faktor üçün bunu demək olar ki, dərin təlim inanılmaz dərəcədə böyük həcmdə məlumat tələb edir.

İkinci faktor üçün bunu demək olar ki, dərin təlim əhəmiyyətli hesablama gücünə ehtiyac duyur. Bununla belə, bulud hesablama infrastrukturunun və yüksək məhsuldarlığa malik prosessorların meydana çıxması ilə dərin təlim şəbəkəsinin təlimi üçün vaxt aylardan həftələrə, həftələrdən saatlara qədər azaldıla bilər.

Dərin təlim sahəsində ən mühüm irəliləyişlərdən biri transfer təliminin meydana çıxması, yəni əvvəlcədən hazırlanmış modellərin istifadə prosesidir. Çünki, təlimin hazır məlumatlardan istifadəsi neyronların dəqiq nəticələr əldə etməsi üçün zəruri olan böyük verilənlər toplularının ehtiyacları üçün köməkçi kimi qəbul edilə bilər.

2.2. Maşın təlimi üsullarının analizi

Maşın təlimi kompüterin təliminə imkan verən alqoritmləri və metodları inkişaf etdirmək, anlamaq və qiymətləndirmək məqsədi daşıyan süni intellekt sahəsidir. Maşın təliminə statistika, insan psixologiyası və beyin modelləşdirmə üsulları daxildir. Beyin modelləşdirməsindən əldə edilən insan psixologiyası və sinir modelləri insan beyninin necə işlədiyini və xüsusən də onun necə öyrəndiyini anlamağa kömək edir ki, bu da maşın təlimi alqoritmlərini formalaşdırmaq üçün istifadə edilə bilər.

Formal olaraq maşın təliminin məqsədi (X) verilənləri (Y) proqnoza çevirən f : X ⇒ Y funksiyasını tapmaqdır. Funksiya müxtəlif təlim alqoritmlərindən ibarət olan müəyyən funksiyalar sinfinə aiddir. Təlim prosesi şəkil 2.3 -də verilmişdir.

Şək. 2.3. Maşın təlimi prosesi (Cəfərov Qiyas, 2024)

Giriş məlumatları və ya təlim dəsti müşahidələrdən, yaddaş anbarlarından və əlavə əsaslandırma üçün faktiki bazadan ibarətdir. Abstraksiya mərhələsində məlumatlar ümumi təsvirlərə çevrilir və məna verilir. Abstrakt əlaqələr biliyin

təsvirinin əsasını təşkil edir. Biliklərin təqdim edilməsində giriş məlumatları verilənlər arasında strukturlaşdırılmış nümunələrin açıq təsviri olan modelə ümumiləşdirilir. Uyğun modelin formalaşdırılması prosesi təlim adlanır (J. B. Fraley and J. Cannady , 2017). Modelin məqsədi təlim məlumatlarını çoxaltmaq deyil, yeni görünməyən nümunələri proqnozlaşdırmaqdır. Modelin yeni hadisələri proqnozlaşdırmaq qabiliyyəti ümumiləşdirmə adlanır. Ümumiləşdirmə hərəkətləri yerinə yetirmək üçün mücərrəd məlumatlardan istifadə edir və modeli tətbiqlər üçün faydalı edir. Bütün mümkün modellər araşdırılsa da, bu mümkün deyil. Beləliklə, öyrədilmədə mümkün nümunələri azaltmaq üçün evristik üsullardan istifadə edilir.

Təlim prosesi ilə bağlı həll edilməli olan bir neçə problem vardır. Məsələn, səhv qoyulmuş məsələnin unikal həlli yoxdur və həll yolları optimal deyil. Buna görə də, eyni məsələnin həlli üçün müxtəlif təlim məlumatları istifadə edildikdə müxtəlif nəticələr alına bilər. Beləliklə, daha çox təlim məlumatları mövcud olduqda, məsələnin nəticəsi daha dəqiq olur.

Məsələnin vahid həllinin olması üçün induktiv meyl adlanan əlavə fərziyyələr olmalıdır. Məsələn, optimallaşdırma kriteriyasının (minimumlaşdırılacaq xəta) seçilməsi induktiv meyldir. Təlim alqoritmlərinin tez-tez istifadə etdiyi verilənlərin induktiv meyli müstəqil və bərabər paylanmış nümunələrdir. Bu nümunələrin hamısı eyni bir birgə paylamadan götürülməlidir.

Müstəqil və eyni şəkildə paylanmış təxmin özünü doğrultmaya bilər, çünki paylanmalar adətən eyni deyil. Bu problemi həll etmək üçün maşın təlimi kovariant sürüşmə fərziyyəsindən istifadə edir. Başqa sözlə, maşın təlimində təlim dəsti və test dəstinin müxtəlif ehtimal paylamalarına malik olduğu güman edilir, lakin giriş qiymətlərinə nisbətən çıxış proqnozlarının paylanması eyni qalır.

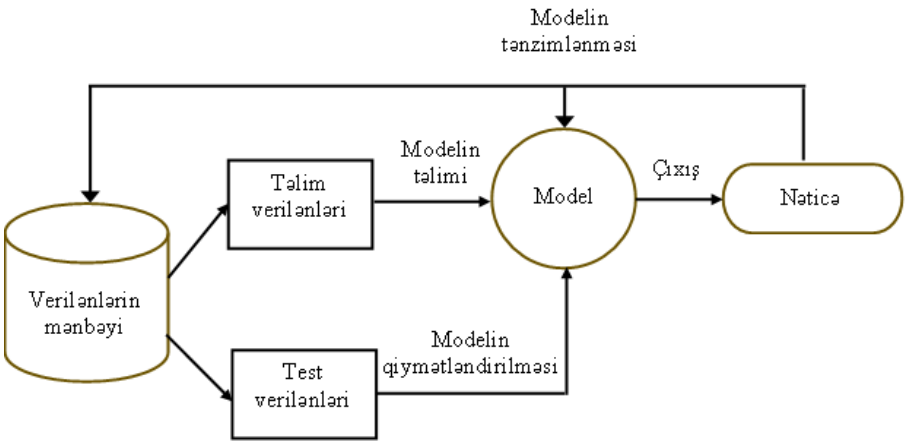
Maşın təlimində həll edilməli olan əsas problem, modelin uyğun olmamasıdır. Model o zaman uyğun olmur ki, onun mürəkkəbliyi verilənləri generasiya edən funksiyanın mürəkkəbliyindən azdır. Başqa sözlə, xətti modelin ümumi çoxhədli funksiyanın köməyi ilə alınmış verilənlərə uyğunlaşdırılması modelin uyğunlaşdırılmasına səbəb olacaq. Digər tərəfdən, model təlim dəstində mükəmməl

nəticələr göstərir, lakin modeli ümumiləşdirə bilmədikdə, bunun həddindən artıq uyğun olduğu deyilir.

Maşın təlimində əsas problemlərdən biri də verilənlərin ölçüsünün çox böyük olmasıdır. Verilənlərin ölçüsünün çox böyük olması zaman və məkan mürəkkəbliyinə təsir edərək, alqoritmlərin yavaş işləməsinə və hesablamaların daha bahalı olmasına gətirib çıxarır. Bu problemi həll etmək üçün ədəbiyyatda verilənlərin ölçülərinin azaldılması üçün müxtəlif üsullar təklif edilmişdir.

Verilənlərin ölçülərinin azaldılması üsulları iki kateqoriyaya bölünür: əlamətlərin seçilməsi və əlamətlərin çıxarılması. Əlamətləri seçərkən ən çox informativ k əlamət seçilir, qalanları isə atılır. Əlamətlərin çıxarılması zamanı ilkin ölçülərin kombinasiyası olan k ölçüsünün yeni dəsti aşkar edilir. Geniş istifadə olunan əlamətlərin çıxarma üsulu əsas komponent analizi adlanır.

Maşın təlimi verilənlərin analizi ilə bağlı məsələlərin həlli üçün müxtəlif alqoritmlərdən istifadə edir. Nəzarət edilən maşın təlimi bir sıra təlim nümunələrindən ibarət etiketlənmiş təlim verilənlərindən xüsusiyyətləri çıxarır. Nəzarət olunan maşın təlimi alqoritmləri xarici yardım tələb edən alqoritmlərdir (S. Dua and X. Du, 2016). Nəzarət olunan maşın təlimi alqoritmlərinin təlim prosesi şəkil 2.4-də göstərilmişdir:

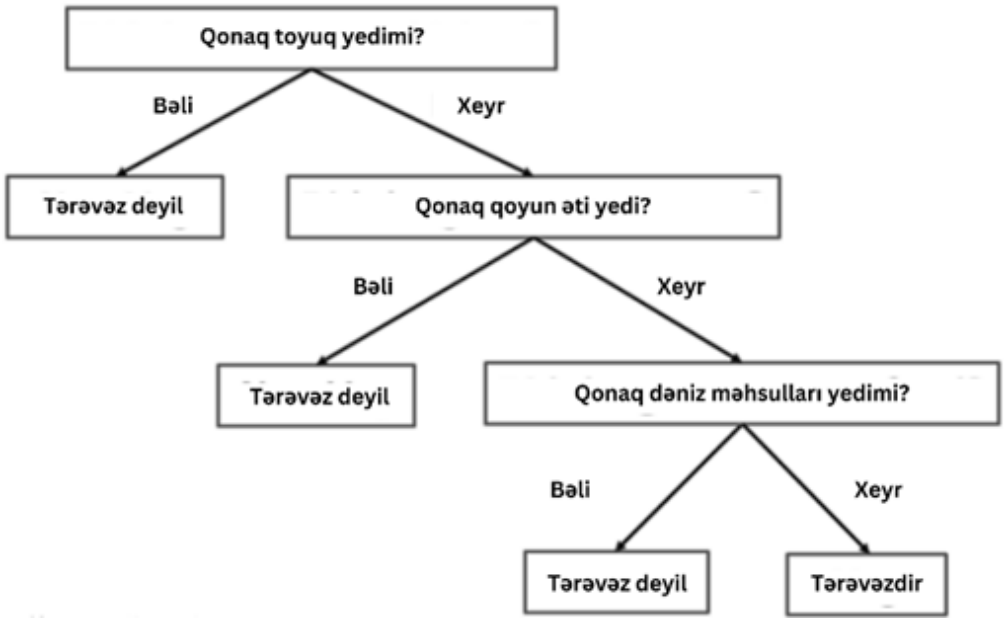


Şək. 2.4. Nəzarət olunan təlim prosesi (Abeshu and N. Chilamkurti, 2018)

Giriş verilənlər bazası iki hissəyə - təlim və sınaq verilənlər bazasına bölünür. Təlim məlumat dəsti proqnozlaşdırılan və ya təsnif olunan çıxış dəyişəninə malikdir. Bütün alqoritmlər təlim məlumat dəstindən müəyyən növ nümunələri öyrənir və onları

proqnozlaşdırma və ya təsnifat məqsədləri üçün test məlumat dəstinə tətbiq edir. Nəzarət edilən təlim maşın təlimi modellərini inkişaf etdirmək üçün təsnifat və reqressiya üsullarından istifadə edir.

Qərar ağacı seçimləri və onların nəticələrini ağac şəklində əks etdirən qrafikdir. Qrafikin qovşaqları hadisə və ya seçimi, qrafikin tilləri isə qərar vermə qaydalarını və ya şərtlərini təmsil edir. Hər bir ağac düyünlərdən və budaqlardan ibarətdir (Şəkil 2.5). Hər bir qovşaq təsnif edilməli olan qrupdakı atributları təmsil edir və hər bir budaq qovşağın ala biləcəyi dəyəri təmsil edir.



Şək. 2.5. Qərar ağacı (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018)

Naive Bayes proqnozlaşdırma məsələlərinin həli üçün nəzərdə tutulmuşdur və Bayes teoreminə əsaslanan təsnifat üsuludur. Naive Bayes klassifikatoru alqoritmi ondan ibarətdit ki, sinifdə müəyyən xüsusiyyətin olması hər hansı digər xüsusiyyətin mövcudluğu ilə əlaqələndirilmir. Naive Bayes əsasən mətnlərin təsnifatında geniş istifadə edilir. Əsasən şərti baş vermə ehtimalı əsasında qruplaşdırma və təsnifat məqsədləri üçün istifadə olunur.

Naive Bayes metodunda fərz edilir ki, x∈ X obyektləri statistik asılı olmayan n əlamətlə təsvir olunur (2.1):

$$X = (\xi_1, \dots, \xi_n) = (f(x_1), \dots, f(x_n)) \quad (2.1)$$

Asılı olmama fərziyyəsi o deməkdir ki, siniflərin həqiqətə oxşarlıq funksiyalarını

$$p_y(x) = p_{y1}(\xi_1) \dots p_{yn}(\xi_n) \quad (2.2)$$

şəklində göstərmək olar, burada y sinfində j-ci əlamətin qiymətlərinin paylanma sıxlığıdır.

Asılı olmama fərziyyəsi məsələni əhəmiyyətli dərəcədə sadələşdirir, çünki birölçülü sıxlıqları qiymətləndirmək, *n* ölçülü paylanma sıxlığını qiymətləndirməkdən daha asandır. Təəssüf ki, bu fərziyyə praktikada nadir hallarda yerinə yetirilir, metodun adı da buradan yaranmışdır. Naive Bayes metodunun qərar qaydası

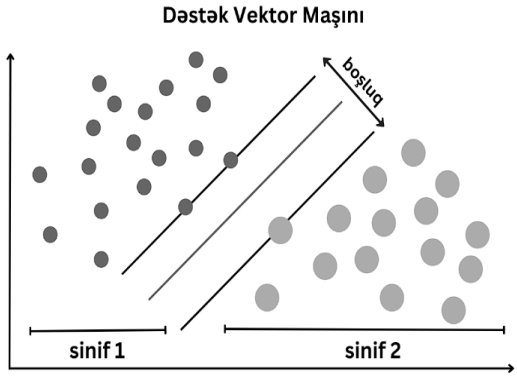
$$h(x) = argmax\ y\epsilon Y \prod_{i=1}^{n} p(x_i|y)p(y) \quad (2.3)$$

şəklindədir. Beləliklə, Naive Bayes təsnifat alqoritminin öyrədilməsi üçün siniflərin p(y) aprior ehtimallarını və $p(x_i|y)$ şərti ehtimallarını qiymətləndirmək lazımdır (S. Yeom, I. Giacomelli, M. Fredrikson, and S. Jha, 2018). **Üstünlükləri**

- Asılı olmayan prediktorlarla bağlı fərziyyə doğru olduqda, Bayes klassifikatoru digər modellərdən daha yaxşı nəticə verir.
- Naive Bayes, test məlumatlarını qiymətləndirmək üçün az miqdarda təlim məlumatı tələb edir. Bu o deməkdir ki, təlim müddəti daha qısadır. Naive Bayes metodunun tətbiqi asandır.

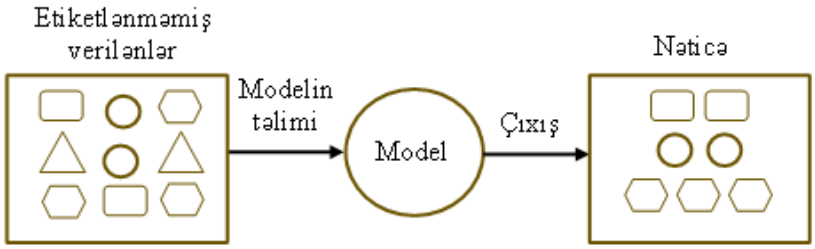
Dəstək Vektor Maşını (DVM) ən çox istifadə edilən müasir maşın təlimi metodlarından biridir. Maşın təlimində dəstək vektor maşını təsnifat və reqressiya analizi üçün istifadə olunan məlumatları analiz edən əlaqəli öyrənmə alqoritmləri ilə nəzarət edilən öyrənmə modelidir. Xətti təsnifatı yerinə yetirməklə yanaşı, DVM-lər böyük ölçülü xüsusiyyət fəzasına daxil olan məlumatların qeyri-xətti olaraq təyin

edilməsi ilə nüvə hiyləsi adlanan üsuldan istifadə edərək qeyri-xətti təsnifatı effektiv şəkildə həyata keçirə bilər (Şəkil 2.6). Əsasən bu, siniflər arasında sərhədlərin çəkilməsindən ibarətdir. Sahələr elə çəkilir ki, sahələr və siniflər arasındakı məsafə maksimuma çatdırılsın və beləliklə, təsnifat xətasını minimuma endirsin.



Şək. 2.6. Dəstək vektor maşını (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018)

Nəzarətsiz təlim nəzarətli təlimdən fərqli olaraq düzgün cavablar yoxdur və müəllim yoxdur və model etiketlənməmiş verilənlərin gizli nümunələrini və ya daxili strukturlarını özü aşkar edir (Şəkil 2.7). Bu zaman, nəzarətsiz təlim modelləri verilənlərdən bir neçə xüsusiyyəti öyrənirlər. Yeni verilənlər daxil edildikdə, verilənlərin sinfini tanımaq üçün əvvəllər öyrənilmiş xüsusiyyətlərdən istifadə edilir. Əsasən klasterləşdirmə və xüsusiyyətlərin azaldılması üçün istifadə olunur (S. Dua and X. Du, 2016).



Şək.2.7. Nəzarətsiz təlim (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018)

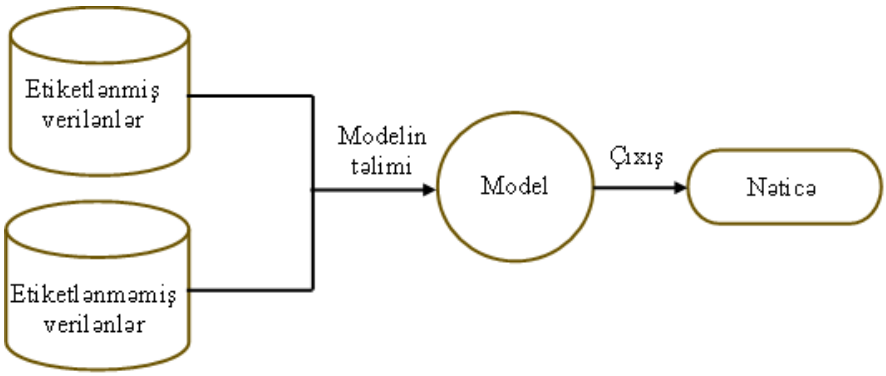
Əsas komponent analizi, ehtimal ki, əlaqəli dəyişənlərin müşahidələri toplusunu əsas komponentlər adlanan xətti əlaqəsi olmayan dəyişənlərin dəyərlərinə

çevirmək üçün ortoqonal çevrilmədən istifadə edən statistik prosedurdur. Eyni zamanda, məlumatların ölçüsü azaldılır, hesablamalar daha sürətli və sadə olur. Xətti birləşmələr vasitəsilə dəyişənlər çoxluğunun dispersiya-kvariasiya strukturunu təsvir etmək üçün istifadə olunur. Tez-tez ölçüləri azaltma usulu kimi istifadə olunur.

K-Means klasterləşdirmə problemini həll edən ən sadə nəzarətsiz təlim alqoritmlərindən biridir. Prosedur müəyyən sayda klasterlər vasitəsilə verilmiş məlumat dəstini təsnif etmək üçün sadə və asandır. Əsas ideya hər klaster üçün bir ədəd olmaqla K mərkəzi müəyyən etməkdir. Bu mərkəzləri elə şəkildə yerləşdirmək lazımdır, ki fərqli yerləşdirmələr fərqli nəticələr versin. Buna görə də, ən yaxşı seçim onları mümkün qədər uzaq yerləşdirməkdir.

Yarı nəzarətli maşın təlimi nəzarət edilən və nəzarətsiz maşın təlimi üsullarının birləşməsidir. Bu təlimd modelin öyrədilməsi üçün həm etiketlənmiş verilənlərdən, həm də etiketlənməmiş istifadə edilir (Şəkil 2.8).

Transduktiv dəstək vektor maşınları (TDVM-lər) yarı nəzarətli təlimdə qismən etiketlənmiş verilənlərin emalı vasitəsi kimi geniş istifadə olunur. O, etiketlənməmiş verilənləri elə etiketləmək istifadə olunur ki, etiketli və etiketsiz verilənlər arasındakı fərq maksimum olsun. TDVM-dən istifadə edərək dəqiq bir həll tapmaq NP çətin bir problemdir (S. Yeom, I. Giacomelli, M. Fredrikson, and S. Jha, 2018).



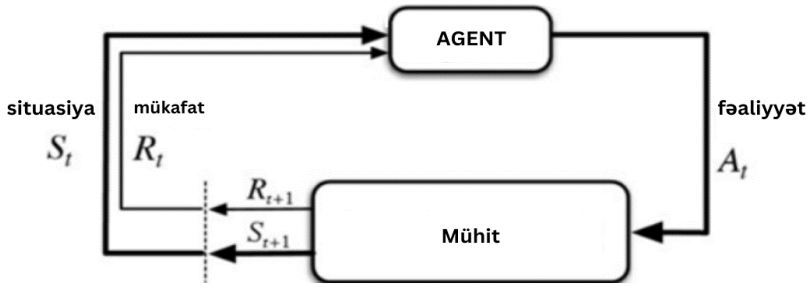
Şək.2.8. Yarı nəzarətli maşın təlimi (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018)

Generativ model verilənləri generasiya edə bilən modeldir. Həm xüsusiyyətləri, həm də sinfi modelləşdirir, yəni verilənlirin tam modelləşdirir. Əgər P(x,y)

modelləşdirilirsə, onda bu ehtimal bölgüsündən verilər nöqtələrini yaratmaq üçün istifadə edilə bilər və buna görə də P(x,y) modelini verən bütün alqoritmlər generativdir. Qarışığın paylanmasını yoxlamaq üçün isə hər komponentə bir etiketlənmiş nümunə kifayətdir.

Öz-özünə təlim zamanı klassifikator etiketlənmiş verilənlər üzrə öyrədilir. Təsnifatlayıcı daha sonra etiketlənməmiş verilənləri alır. Etiketlənməmiş nöqtələr və proqnozlaşdırılan etiketlər təlim dəstində toplanır. Bu prosedur daha sonra təkrarlanır. Təsnifatlayıcı özü öyrəndiyi üçün öz-özünə təlim adı verilir.

Gücləndirici təlim proqram agentlərinin mühitdə məcmu mükafatı artırmaq üçün necə hərəkət etmələri ilə məşğul olan maşın təliminin bir növüdür (Şəkil 2.9). Gücləndirici təlim nəzarət edilən təlim və nəzarətsiz təlim ilə birlikdə üç əsas maşın təlim paradiqmasından biridir.



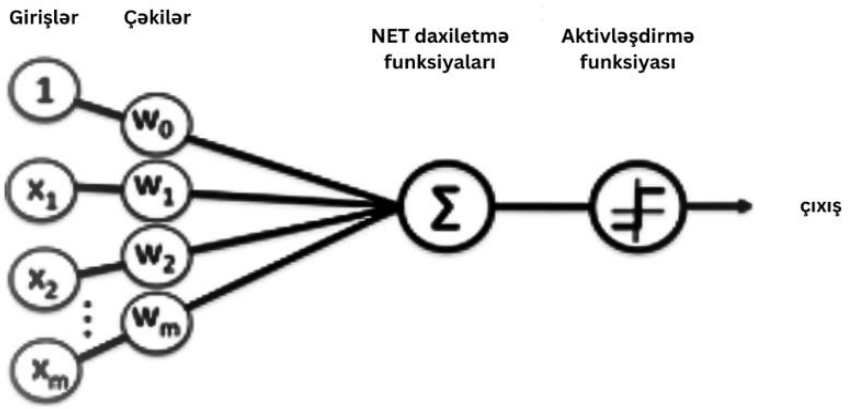
Şək. 2.9. Gücləndirici təlim (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018)

Çox məsələli təlim, müxtəlif məsələlər arasındakı oxşarlıqlardan istifadə edərək eyni vaxtda bir neçə fərqli problemi həll etməyi qarşısına məqsəd qoyan maşın təliminin alt sahəsidir. Bu, təlim səmərəliliyini artıra bilər və həm də nizamlanma kimi çıxış edə bilər. Formal olaraq, əgər n məsələ varsa, çox məsələli təlim bu n məsələnin və ya onların bir hissəsinin əlaqəli olduğu bütün n problemdə özünü göstərir. Lakin bu bütün məsələrdə tam olaraq eyni olmur.

Ansambl təlimi xüsusi hesablama intellekt problemini həll etmək üçün təsnifatçılar və ya ekspertlər kimi çoxsaylı modellərin yaradıldığı və strateji şəkildə birləşdirildiyi bir prosesdir. Ansambl təlimi ilk növbədə modelin məhsuldarlığını yaxşılaşdırmaq və ya pis modelin seçməsi ehtimalını azaltmaq üçün istifadə olunur.

Ansambl təliminin digər tətbiqlərinə model tərəfindən verilən qərara inamın təmin edilməsi, optimal xüsusiyyətlərin seçilməsi, məlumatların birləşdirilməsi, müvəqqəti təlim və səhvlərin düzəldilməsini özündə birləşdirir.

Neyron şəbəkəsi insan beyninin fəaliyyətini təqlid edən bir proses vasitəsilə verilənlər toplusunda əsas əlaqələri tanımağa çalışan alqoritmlər toplusudur. Bu mənada neyron şəbəkələri təbiətcə süni olan sinir sistemlərinə aiddir. Neyron şəbəkələr daxil olan verilənlərindəki dəyişikliklərə uyğunlaşa bilir. Bu şəkildə şəbəkə çıxış meyarlarını yenidən nəzərdən keçirmədən mümkün olan ən yaxşı nəticəni verir. Sadə süni neyron şəbəkəsi üç laydan ibarətdir (Şəkil 2.10). Giriş layı giriş verilənlərini qəbul edir. Gizli lay daxil edilən verilənləri emal edir. Nəhayət, çıxış layı hesablanmış nəticəni göndərir (S. Yeom, I. Giacomelli, M. Fredrikson, and S. Jha, 2018).



Şək. 2.10. Neyron şəbəkəsi (Raymond O. Kene 2023)

Maşın təlimi üsullarının qiymətləndirilməsi

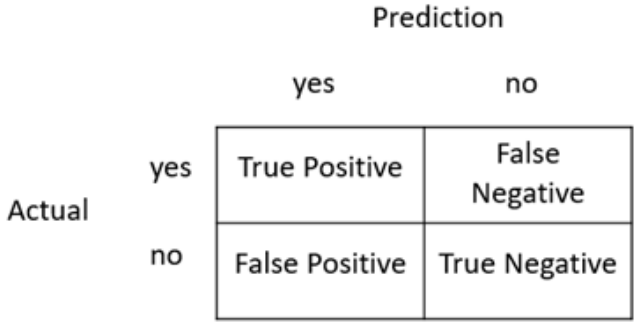
Maşın təlimi üsullarının qiymətləndirilməsinin məqsədi üsulların nəticələrini verilmiş məsələ üzrə digər üsullarla müqayisə edilməsidir. Qiymətləndirmənin ümumi ideyası verilənlərin təlim, yoxlama və test dəstlərinə bölməkdir. Maşın təlimi üsulu təlim dəstindən istifadə etməklə öyrədilir, gözlənilən xətanı əldə etmək üçün yoxlama dəsti üzərində sınaqdan keçirilir və nəhayət, metodun real vəziyyətdə necə işləyəcəyini görmək üçün test dəsti istifadə olunur.

Təsnifat məsələsində maşın təlimi üsulunun nə qədər yanlış olduğunu qiymətləndirmək üçün çarpaz yoxlama istifadə olunur. Bunun üçün təlim verilənləri K hissələrinə bölünür və sonra yenidən təlim dəstinə və metodu sınaqdan keçirmək üçün

istifadə olunacaq test dəstinə bölünür. Həmçinin, k-qat çarpaz yoxlama təlim verilənlərini eyni ölçülü K dəstlərinə bölür. Bir dəst test dəsti kimi, digərləri isə təlim dəsti kimi istifadə olunur (K-1 ölçüsü). Sonra bu təkrarlanır və hər bir bölünmə bir dəfə test dəsti olsun, bu da K təkrarlanma sayını verir. Səhvlər toplanır və orta qiymət hesablanır.

Təsnifat məhsuldarlığını qiymətləndirmək üçün qarışıqlıq matrisi istifadə edilir (Şəkil 2.11). Qarışıqlıq matrisi düzgün və səhv nişanlanmış nümunələrin nömrələrini göstərən bir cədvəldir və aşağıdakı hissələrdən ibarətdir:

- True Positive (TP): müsbət nümunə kimi düzgün proqnoz;
- True Negative (TN): mənfi nümunə kimi düzgün proqnoz;
- False positive (FP): müsbət nümunə kimi yanlış proqnozlaşdırılır;
- False negative (FN): mənfi nümunə kimi yanlış proqnozlaşdırılır.



Şək. 2.11. Qarışıqlıq matrisi (Roni Andarsyah, 2023)

Bundan əlavə, bir çox ölçülər qarışıqlıq matrisindən əldə edilir və təsnifatçının işini qiymətləndirmək üçün istifadə olunur:

- **Dəqiqlik (Accuracy)** klassifikatorun düzgün proqnozları nə qədər tez-tez edəcəyini göstərir. Dəqiqlik, düzgün proqnozların sayı ilə ümumi proqnozların sayı arasındakı nisbətdir.
- **Dürüstlük (Precision)** klassifikatorun düzgünlüyünü ölçür, geri qayıdan sənədlərin neçə faizinin düzgün olduğunu göstərir. Daha yüksək dürüstlük daha az yalan pozitiv, daha aşağı dürüstlük isə daha çox yalan pozitiv deməkdir. Dürüstlük, düzgün təsnif edilən nümunələrin ümumi nümunələrə olan nisbətidir.

- **Doğruluq (Recall)** klassifikatorun həssaslığını hesablayır, yəni müsbət məlumatları qaytarma qabiliyyətini ölçür. Daha yüksək doğruluq daha az yalan neqativ deməkdir. Doğruluq, dəqiq təsnif edilmiş müsbət nümunələrin ümumi müsbət nümunələrə olan nisbətidir.
- **F-score** dürüstlük və doğruluğun ortaölçülü harmonik qiymətidir.

Dəqiqlik düzgün proqnozlaşdırılan nümunələrin nisbətini göstərir. Beləliklə, dəqiqlik aşağıdakı kimi müəyyən edilir:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FP} \quad (2.4)$$

Əksər tətbiqlərdə ancaq dəqiqlik ən güclü məhsuldarlıq göstəricisidir. Bununla belə, elə məsələlər var ki, onların dəqiqliyi təsnifatçının məhsuldarlığını göstərə bilmir, ona görə də əlavə məhsuldarlıq ölçülməsinə ehtiyac var. Sentiment təhlildə dürüstlük (precision) və dolğunluq (recall) geniş istifadə edilir. Dürüstlük, modelin nə qədər etibarlı ola biləcəyini ifadə edir və əslində müsbət nümunələrin nisbətini ölçür (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018).

Dürüstlük aşağıdakı kimi müəyyən edilir:

$$Precision = \frac{TP}{TP + FP} \quad (2.5)$$

Digər tərəfdən, doğruluq (recall) müsbət nümunələrin ümumi sayında düzgün nişanlanmış nümunələrin nisbətinin nə qədər yüksək olduğunu göstərir:

$$Recall = \frac{TP}{TP + FN} \quad (2.6)$$

Başqa bir ölçü, dolğunluq (recall) və dürüstlüyün (precision) harmonik ortalaması olan F-score-dur və aşağıdakı kimi müəyyən edilir::

$$F = \frac{2 * Precision * Recall}{Precision + Recall} \quad (2.7)$$

Verilmiş $C = \{c_1 \dots c_{|C|}\}$ təsnifat məsələsinin bütün siniflərinin çoxluğudur. Macro_P ölçüsü, C dəstindəki bütün siniflər üçün dürüstlük (precision) dəyərlərinin arifmetik ortalamasıdır:

$$Macro\_P = \frac{1}{|C|} * \sum_{\forall i:\, c_i \in C} precision(c_i) \quad (2.8)$$

Macro_R dəyəri də eyni şəkildə daxil edilir. Macro_R ölçüsü C dəstindəki bütün siniflər üçün Recallın dəyərlərinin arifmetik ortasıdır:

$$Macro\_R = \frac{1}{|C|} * \sum_{\forall i:\, c_i \in C} Recall(c_i) \quad (2.9)$$

Məhsuldarlığın qiymətləndirilməsi üçün ümumi vizuallaşdırma vasitəsi ROC (receiver operating characteristic) əyrisidir. ROC əyrisi aşkarlama arasındakı uyğunluğu göstərir. Əksər təsnifatçılar ideal təsnifatçı və heç bir proqnoz dəyəri olmayan təsnifatçı arasında olur. Təsnifatçının doğru müsbət və yalan müsbət nisbətləri ilə ideal təsnifatçıya nə qədər yaxın olduğunu görmək üçün adətən ROC əyrisinin altındakı sahə (AUC - area under the curve) ölçüsü hesablanır (Géron, A. , 2019).

2.3. Dərin təlim üsullarının analizi

Həm maşın təliminin, həm də süni intellektin bir hissəsi olan dərin təlim, biliklərin xüsusi formalarını əldə etmək üçün insanın təlim proseslərini təqlid edir. Dərin təlimdə 'dərin' termini, şəbəkəyə iyerarxik məlumat təqdimatlarını qavramağa imkan verən çoxsaylı gizli layların mövcudluğunu bildirir.

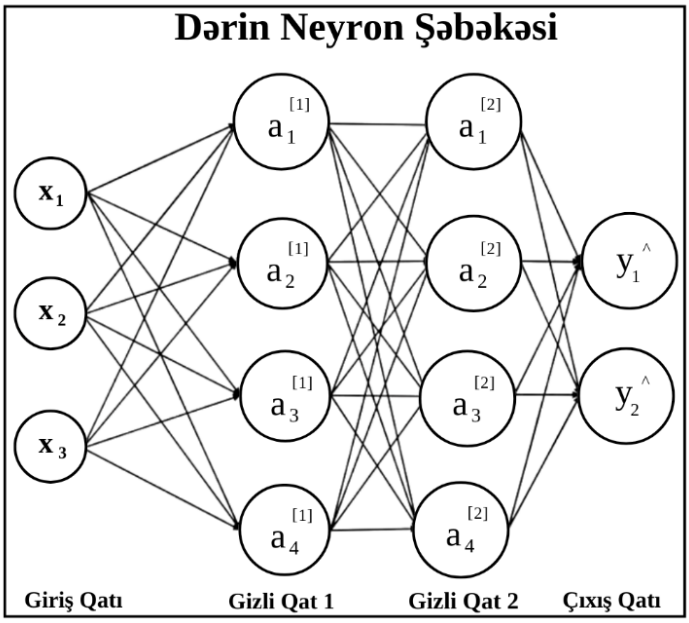
İnsan beynindəki neyronlar tərəfindən elektrik impulslarının ötürülməsinin analoqu kimi, dərin təlimdə olan perseptronlar bir sıra giriş siqnallarını qəbul edir və onları çıxış siqnallarına çevirir. Perseptronların hər bir layı verilənlər bazasında xüsusi nümunələri deşifrə etmək tapşırığını daşıyır.

Dərin təlim ənənəvi maşın təlimi üsulları ilə bağlı məhdudiyyətləri həll etmək üçün geniş imkanlar təqdim edir. Ənənəvi maşın təlimi xüsusiyyət çıxarma vəzifəsi fərdlər tərəfindən əl ilə yerinə yetirilir. Buna baxmayaraq, geniş məlumat dəstlərinin idarə edilməsinə gəldikdə, dərin neyron şəbəkələri insan imkanlarını üstələyən xüsusiyyətlər çıxarmaqda üstündür (Imamverdiyev Y, Abdullayeva F, 2018).

2.3.1. Dərin təlim

Dərin neyron şəbəkənin komponentlərinə aşağıdakılar daxildir:

- Giriş layı: Bu lay giriş məlumatlarını qəbul edən və onu neyron şəbəkənin sonrakı laylarına ötürən qovşaqlardır.
- Gizli lay: Bu lay alınan məlumatları müxtəlif səviyyələrdə emal edir.
- Çıxış lay: Bu lay son nəticələr və ya proqnozlar verən qovşaqlardan ibarətdir. Binar təsnifat tapşırıqlarında çıxış qatında iki qovşaq ola bilər. Şəkil 2.12-də iki gizli laydan ibarət Dərin Neyron Şəbəkəsi qeyd olunub (Abeshu and N. Chilamkurti, 2018).



Şək. 2.12. İki gizli laydan ibarət dərin neyron şəbəkəsi (Tony Beltramelli, 2015)

Kibertəhlükəsizlikdə dərin təlimin tətbiqinin bəzi əsas üstünlükləri bunlardır:

- Avtomatlaşdırılmış cavab
- Fişinq aşkarlanması
- Zərərli proqramdan mühafizə
- Şəbəkə təhlükəsizliyi
- Yanlış pozitivlərin azaldılması
- Xərc effektivliyi

Dərin təlimin tətbiq sahələri

- Vizual Tanınma: Smartfonlarda və sosial media platformalarında üz tanıma funksiyası kimi sifətin aşkarlanması, obyektin identifikasiyası və təsvirin bölünməsi kimi vəzifələrə kömək edir.

- Təbii dilin email (NLP): Dil tərcüməsi, hisslərin təhlili və mətnin sıxlaşdırılması kimi NLP səylərində çatbotlar mühüm rol oynayır, sorğulara cavab verə və müştəri dəstəyi təklif edə bilərlər.

- Nitq Tanınması: Siri, Alexa və Google Assistant kimi səslə aktivləşdirilən axtarış və virtual köməkçilərin yaradılmasında iştirak edir.

- Tövsiyə Sistemləri: İstifadəçi seçimlərinə əsaslanaraq elementləri və ya məzmunu tövsiyə etməklə tövsiyə sistemlərini təkmilləşdirir. Netflix və Amazon buna misaldır.

- Fırıldaqçılığın Aşkarlanması: Dərin təlim, kredit kartı fırıldaqları və şəxsiyyət oğurluğu kimi davranışların müəyyən edilməsində mühüm rol oynayır. Banklar şübhəli əməliyyatları aşkar etmək üçün dərin təlimdən istifadə edirlər.

- Avtonom Nəqliyyat Vasitələri: Dərin təlim, özü idarə edən nəqliyyat vasitələrinə ətrafda naviqasiya etməkdə və maneələrdən qaçmaqda kömək edir. Bu, onlara yol nişanlarını və piyadaları tanımağa imkan verir.

- Əczaçılıq Tədqiqatı: Dərman namizədlərinin effektivliyini proqnozlaşdırmaqla dərman kəşfini asanlaşdırır. Əczaçılıq şirkətləri müxtəlif xəstəliklərin müalicəsi üçün ondan istifadə edirlər.

- İqlim Modelləşdirilməsi: İqlim dəyişikliyinin təsiri nəticəsində dəniz səviyyələrində və hava modellərində baş verən dəyişiklikləri proqnozlaşdırmaq üçün istifadə olunur (He, K., & Kim, D. S. , 2019).

2.3.2 Dərin təlim yanaşmalarının təsnifatı

Dərin təlim yanaşmaları müxtəlif meyarlara əsasən müxtəlif kateqoriyalara təsnif edilə bilər (Şəkil 2.13):

Təlim növünə görə:

- Nəzarət olunan təlim. Girişlər və arzu olunan çıxışlar arasındakı əlaqəni öyrənərək etiketlənmiş verilənlər əsasında modellər yaradılır. Təsvirin təsnifatı, əhval-ruhiyyənin analizi və s. məsələlərinin həlli üçün istifadə edilir.

- Nəzarətsiz təlim. Etiketlənməmiş verilənlərdən istifadə edərək, verilənlərin özündə nümunələri müəyyən edir. Anomaliyaların aşkarlanması, ölçülərin azaldılması və s. məsələlərinin həlli üçün istifadə edilir.

Modelin arxitekturasına görə:

- Konvulyasiya Neyron Şəbəkəsi (CNN): Ölçülərin azaldılması elementlərin alınması və birləşən laylar üçün konvolyusiya qatlarından istifadə edilir.

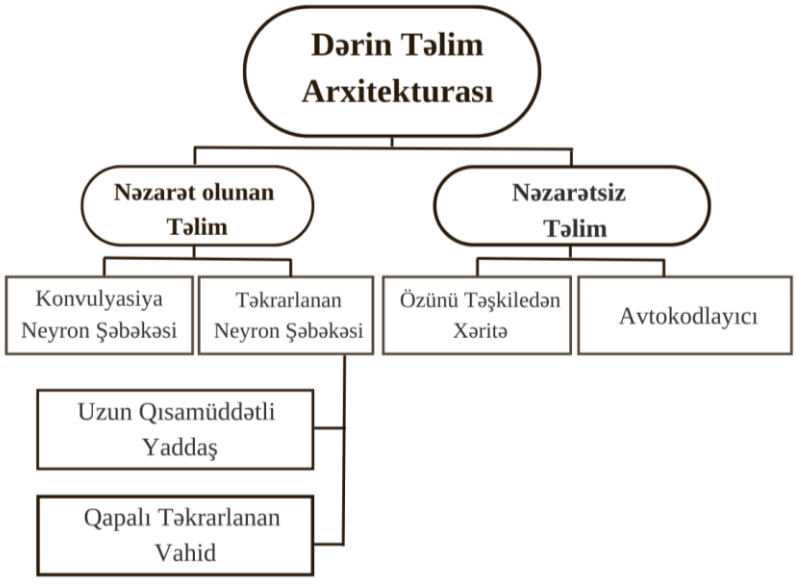
- Təkrarlanan Neyron Şəbəkəsi (RNN): Mətn və ya nitq kimi məlumat üçün nəzərdə tutulmuşdur. Əvvəlki addımlardakı ödəniş saxlayaraq daxil olun-addım emal edir.

- Uzun Qısa müddəti Yaddaş Şəbəkəsi (LSTM): Ənənəvi RNN-lərdə yoxa çıxan gradient problemini həll edir. Maşın tərcüməsi kimi uzun məlumatlılığını göstərmək üçün effektivdir.

- Özünü təşkil edən xəritə (SOM): Yüksək ölçülü məlumatların ölçülərinin azaldılması, klasterləşdirilməsi və vizuallaşdırılması kimi vəzifələr üçün istifadə edilə bilər.

- Avtoenkoder: Bu modellər sıxışdırılmış təsviri, eyni zamanda sıxışdırılmış versiyadan asılı məlumatı rekonstruksiya etmək üçün istifadə olunur. O, ölçüsünü azaltma, anomaliyanı aşkar etmə və məlumat əldə etmək kimi məqsəd üçün faydalıdır.

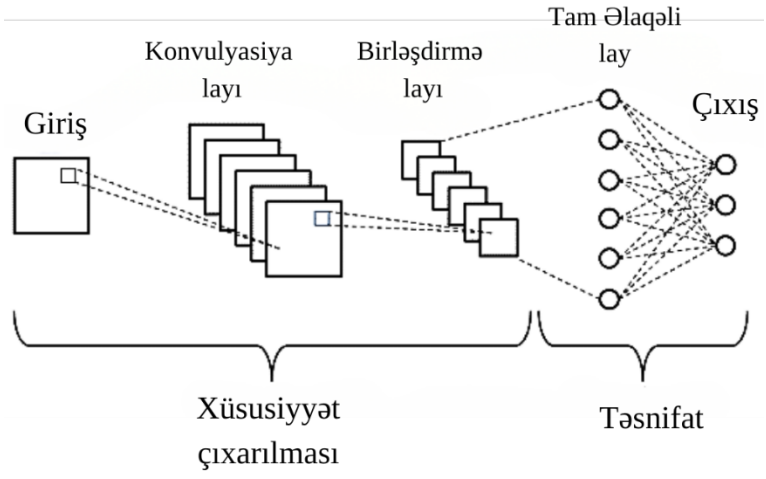
- Qapalı Təkrarlanan blok (GRU): LSTM-lərin arxitekturasını sadələşdirir, nəticədə daha az parametr və daha sürətli təlim vaxtları olur (L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, 2018).



Şək.2.13. Dərin təlim yanaşmalarının təsnifatı
(Aytən Hüseynova, Elnur İbrahimov, 2024)

Konvulyasiya neyron şəbəkəsi (CNN)

CNN-lər adətən geri yayılma alqoritmindən istifadə etməklə öyrədilir. Bu prosesdə şəbəkə parametrləri ilə bağlı itki funksiyasının gradientləri hesablanır və stokastik gradient enməsi kimi optimallaşdırma üsulları vasitəsilə çəkilər yenilənir. Şəkil 2.14-də göstərildiyi kimi, CNN alternativ konvolyusiya və birləşmə qatlarından ibarətdir. Konvulyasiya qatları xüsusiyyətləri çıxarmaq üçün, birləşmə qatları isə xüsusiyyətlərin ümumiləşdirilməsini artırmaq üçün istifadə olunur. CNN-lər 2 ölçülü (2D) məlumatlar üzərində işləyir, buna görə də daxil olan məlumatlar hücumun aşkarlanması üçün matrislərə çevrilməlidir (Zhang, H., Yu, X., Ren, P., Luo, C., Min, G., 2019).



Şək.2.14. CNN-nin strukturu (Alam Moudud, 2022)

Konvulyasiya layı CNN-in əsas tikinti blokudur və daxil edilmiş təsvirlə öyrənilə bilən filtrlər dəsti arasında konvolyusiya əməliyyatını həyata keçirir. Hər bir filtr daxil edilmiş təsvirin üzərində sürüşərək filtr və həmin anda nəzərdən keçirilən təsvirin yerli bölgəsi arasında nöqtə hasilini hesablayır. Bu əməliyyatın nəticəsi, giriş təsvirindəki nümunələrin və ya xüsusiyyətlərin mövcudluğunu vurğulayan xüsusiyyət xəritəsidir. Təlim vasitəsilə müvafiq filtr çəkilərini öyrənməklə, CNN kənarlar,

fakturalar və ya obyekt hissələri kimi giriş məlumatlarından avtomatik olaraq lazımi xüsusiyyətləri çıxara bilər.

Pooling layı, konvolyasiya layını izləyən və vacib məlumatları saxlamaqla xüsusiyyət xəritələrinin məkan ölçülərini azaltmağa xidmət edən birləşdirici qatdır. Bu qat, öyrənilmiş xüsusiyyətləri kiçik məkan tərcümələrinə və girişdəki təhriflərə qarşı daha invariant etməyə kömək edir və eyni zamanda şəbəkənin hesablama mürəkkəbliyini azaldır (Potluri, S.; Ahmed, S.; Diedrich, C., 2018).

Birləşmənin iki əsas növü var:

- Maksimum birləşdirmə: Filtr giriş üzərində hərəkət etdikcə, hər bir bölgə daxilində maksimum dəyəri seçir və onu çıxış massivinə ötürür.
- Orta birləşdirmə: Hər bir bölgə daxilində orta dəyəri hesablayır və onu çıxış massivinə ötürür. Orta birləşdirmə, hesablama mürəkkəbliyini azaldarkən faydalı ola bilər.

Maksimum birləşdirmə, aktivləşdirmə xəritəsində göstərilən hər bir alt pəncərədə maksimum dəyəri çıxarır və 2.10-dakı düsturla müəyyən edilir:

$$A_{i,j,k} = max\left(R_{i-n:i+n,j-n:j+n,k}\right) \qquad (2.10)$$

burada *R* bir xüsusiyyət xəritəsini ifadə edə bilər, *ni* və *nj* isə maksimum-birləşdirmə pəncərəsinin ölçülərini göstərir. Bu halda, *Ai,j,k* əməliyyatdan sonra *k*-cı xüsusiyyət xəritəsindəki (*i,j*) indeksli elementin dəyərini ifadə edir.

Birləşdirmə layının məqsədləri:

- Məkan ölçülərinin və mürəkkəbliyin azaldılması
- Modelin görünməyən məlumatlara ümumiləşdirilməsi
- Xüsusiyyətlərin ümumiləşdirilməsi

Tam əlaqəli lay, ənənəvi neyron şəbəkəsi layıdır, burada hər bir neyron əvvəlki və sonrakı laylardakı hər bir neyronla əlaqələndirilir. Bu lay, konvolyusiya və birləşmə layları tərəfindən çıxarılan yüksək səviyyəli xüsusiyyətləri götürür və onlardan təsnifat və ya reqressiya tapşırıqları üçün istifadə edir.

Tam əlaqəli lay, ehtimala əsaslanan çıxışlar yaratmaq üçün 2.11-dəki softmax düsturu kimi aktivləşdirmə funksiyalarından istifadə edir. Bu, şəbəkədə öyrənilən xüsusiyyətlər əsasında girişləri müxtəlif kateqoriyalara təsnif etməyə imkan verir. Softmax-a əsasən, verilmiş hər bir neyronun çıxışı (z) 0 ilə 1 arasında normalizasiya edilir və hər bir sinifə aid olma ehtimalı hesablanır.:

$$\sigma(z)_j = \frac{e^{z_j}}{\sum_{k=1}^{K} e^{z_k}}, (2.11)$$

burada e Eyler ədədi olub, təbii logarifm funksiyasının bazasıdır, z_j neyronun j-ci çıxışının xam çıxışıdır, K neyronların ümumi iştirakıdır, $\sigma(z)_j$ j-ci elementinin dəyəridir, hansı ki, z vektorunun j-ci komponenti üzərində softmax tətbiq edildiyi zaman alınan ehtimaldır, e^{z_j} z_j komponentinin eksponentini ifadə edir və $\sum_{k=1}^{K} e^{z_k}$ 1-K intervalındakı z_k-nın eksponentlərinin cəmidir (Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S., 2019).

Girişin çıxışa çevrilməsi, bütün növ neyron şəbəkələrində aktivasiya funksiyasının əsas metodur. CNN arxitekturasında, çəkiyə malik olan bütün laylardan sonra qeyri-xətti aktivasiya layları işə salınır. Aktivasiya funksiyası, şəbəkəni təlim etmək üçün geri yayılma xətasından istifadə etməyə imkan verdiyi üçün diferensiallaşdırma qabiliyyətinə malik olmalıdır. Bu xüsusiyyət onu çox əhəmiyyətli edir.

Konvulyasiya laylarında 2.12-dəki düstur bir neyronun və ya qatın aktivasiya dəyərini hesablamaq üçün istifadə olunur:

$$h^k = f(W^k * x + b^k), \quad (2.12)$$

burada h^k: k-cı laydakı neyronların aktivasiya dəyərlərini ifadə edir, f aktivasiya funksiyasıdır, giriş siqnalını qəbul edib çıxış siqnalını verir, W^k k-cı qatdakı ağırlıq matrisidir, öncəki layın aktivasiyaları ilə vurularaq yeni layın aktivasiyalarını hesablamak üçün istifadə olunur, x giriş vektoru və ya öncəki layın aktivasiya dəyəridir, b^k k-cı qatdakı bias vektorudur, ağırlıqla vurulmuş aktivasiyaların üzərinə əlavə edilərək çıxış dəyərlərinin tənzimlənməsində istifadə olunur.

Aşağıda aktivasiya funksiyaları qeyd olunub:

- Siqmoid: 2.13-dəki formulda göstərilən siqmoid funksiyası, məsələn, ikili təsnifat üçün son çıxış qatında giriş dəyərlərini x-a uyğunlaşdırmaq üçün istifadə olunur. Bu funksiya S-şəkilli bir əyriyə malikdir və dəyərləri əsasən [0, 1] diapazonunda dəyişir:

$$f(x)_{sigm} = \frac{1}{1+e^{-x}} \qquad (2.13)$$

- Tanh: Tanh funksiyasının 2.14-dəki düsturda göstərildiyi kimi dəyərləri [-1, 1] diapazonunda dəyişir, məlumatı normallaşdırmaq və məhdudlaşdırmaq üçün istifadə edilə bilər:

$$f(x)_{tanh} = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}}, \quad (2.14)$$

burada x giriş dəyişəni, e isə Eksponent əsası, təxminən 2.71828 dəyərinə bərabər olan sabitdir

- ReLU: 2.15-dakı düsturda göstərilən ReLU funksiyası girişin bütün dəyərlərini müsbət ədədlərə çevirir. Aşağı hesablama yükü ReLU-nun digərlərindən əsas üstünlüyüdür:

$$f(x)_{ReLU} = max(0, x), \qquad (2.15)$$

burada x giriş dəyişəninin dəyəridir (Yin C, Zhu Y, Fei J, He X, 2017).

Konvulyasiya prosesi üçün müəyyən ölçülü aktivləşdirmə xəritələrini hazırlamaq üçün bəzi məkan arqumentləri müəyyən edilməlidir:

- Nüvələrin ölçüsü (N): Hər bir nüvənin bir pəncərə ölçüsü var ki, bu da qəbuledici sahə adlanır. Nüvə, girişdən pəncərə ölçüsünə uyğun bir bölgə ilə konvolyasiya əməliyyatını yerinə yetirir və aktivləşdirmə xəritəsində nəticələr verir.
- Addım (S). Bu parametr nüvənin növbəti mövqeyə keçəcəyi piksellərin sayını müəyyən edir. Əgər 1-ə təyin edilərsə, hər bir nüvə giriş həcmi ətrafında konvolyasiya əməliyyatları aparacaq və sonra girişin müəyyən edilmiş sərhədinə çatana qədər hər dəfə 1 piksel irəliləyəcək. Beləliklə, addım ölçüsü aktivləşdirmə xəritələrinin ölçüsünü azaltmaq üçün istifadə edilə bilər, çünki addım ölçüsü nə qədər böyükdürsə, aktivləşdirmə xəritələri bir o qədər kiçik olur.
- Sıfır doldurma (P). Bu parametr girişin sərhədi ətrafında neçə sıfırın doldurulmasını təyin etmək üçün istifadə olunur, giriş ölçüsünü qorumaq üçün çox faydalıdır.

CNN-nin nətbiq sahələri:

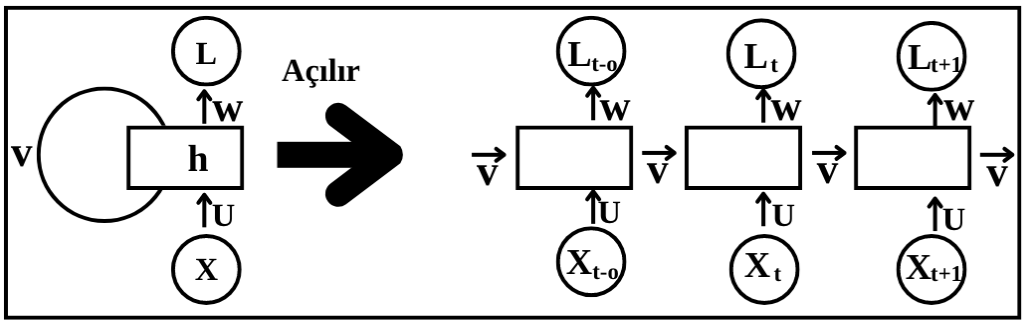
- Şəklin tanınması: Təsvirin təsnifatı tapşırıqları üçün geniş istifadə olunur, burada onlar şəkillərdəki obyektləri, səhnələri və ya nümunələri dəqiq müəyyən edə bilirlər. Tətbiqlərinə üz tanıma, obyekt aşkarlanması və tibbi təsvirin təhlili daxildir.
- Video Analizi: Hərəkətlərin və ya hadisələrin aşkarlanması və təsnifləşdirilməsi üçün hərəkət tanınması, video nəzarət kimi video tanınma tapşırıqlarına tətbiq oluna bilər.
- Təbii Dil Emalı: Mətn məlumatlarını 1D siqnalları kimi nəzərdən keçirmək və konvolyusiya əməliyyatları tətbiq etməklə mətnin təsnifatı, əhval-ruhiyyə təhlili və dil tərcüməsi kimi müəyyən təbii dil emalı tapşırıqlarına da tətbiq oluna bilər.

Rekurent neyron şəbəkələri (RNN)

RNN əks əlaqə dövrələrini daxil etməklə ardıcıl verilənlərin analiz edilməsi üçün nəzərdə tutulmuş rekurent neyron şəbəkəsi arxitekturaları sinfidir. Bu, əvvəlki

addımın çıxışının cari addıma giriş kimi verildiyi neyron şəbəkə növüdür. Beləliklə, RNN-dəki hər bir vahid kontekstual məlumat əldə etmək üçün yalnız cari vəziyyəti deyil, həm də əvvəlki vəziyyətləri alır. Çıxışı əldə etmək üçün bütün girişlərdə və ya gizli laylarda eyni tapşırığı yerinə yetirmək üçün hər bir giriş üçün eyni parametrlərdən istifadə edilir. Bu, digər neyron şəbəkələrdən fərqli olaraq, parametrlərin mürəkkəbliyini azaldır.

RNN-nin strukturu Şəkil 2.15-də göstərilmişdir və burada bütün W elementləri eynidir. Bu xüsusiyyət, RNN-lərin tez-tez yoxa çıxan və ya partlayan gradientlərdən əziyyət çəkməsinə səbəb olur. Əslində, standart RNN-lər yalnız məhdud uzunluqlu ardıcıllıqları analiz edir. Uzunmüddətli asılılıq problemini həll etmək üçün ədəbiyyatda uzun qısamüddətli yaddaş (LSTM) və qapalı təkrarlanan vahid (GRU) kimi RNN variantları təklif edilmişdir (M. Kebede, O. Djaneye-Boundjou, B. N. Narayanan, A. Ralescu, and D. Kapp, 2015).



Şək. 2.15. Rekurent neyron şəbəkəsinin strukturu (M. Saqib Nawaz, 2021)

Rekurent neyron şəbəkələri siqnal emal davranışına görə fərqləndirilə bilən iki alt sinfə malikdir. Birincisi sonlu impulslu təkrarlanan şəbəkələrə (FRN), ikincisi isə sonsuz impulslu təkrarlanan şəbəkələrə (IIRN) aiddir. Bu fərq ondan ibarətdir ki, FRN vaxtında açıla bilən və irəli yayılma neyron şəbəkəsi ilə əvəz edilə bilən yönəldilmiş asiklik qrafik (DAG) ilə təmsil olunur, halbuki IIRN istiqamətləndirilmiş tsiklik qrafikdir (DCG) (Yin C, Zhu Y, Fei J, He X, 2017).

RNN-lər ardıcıl məlumatlar üçün uyğunlaşdırılmış standart geri yayılma alqoritminin bir variantı olan zamanla geri yayılma (BPTT) üsulundan istifadə edərək öyrədilə bilər. BPTT, zamanla şəbəkəni açmağı, onu bir neçə zaman addımı ilə irəli

yayılma şəbəkəsi kimi nəzərdən keçirməyi və sonra gradientləri hesablamaq və çəkiləri yeniləmək üçün standart geri yayılma tətbiq etməyi əhatə edir.

Cari vəziyyəti hesablamaq üçün 2.16-dakı düsturdan istifadə edilir:

$$h_t = f(h_{t-1}, x_t), \quad (2.16)$$

burada h_t cari vəziyyət, h_{t-1} əvvəlki vəziyyət və x_t isə giriş vəziyyətidir.

Aktivləşdirmə funksiyasının tətbiqi 2.17-dəki tanh düsturunda qeyd olunub:

$$h_t = tanh(W_{hh}h_{t-1} + W_{xh}x_t), \quad (2.17)$$

burada W_{hh} təkrarlanan neyronun çəkisi və W_{xh} isə giriş neyronun çəkisidir.

Şəbəkənin çıxışı 2.18-dəki düsturla hesablana bilər:

$$y_t = W_{hy}h_t, \quad (2.18)$$

burada y_t çıxış və W_{hy} isə çıxış layının çəkisidir.

RNN-nin tətbiq sahələri:

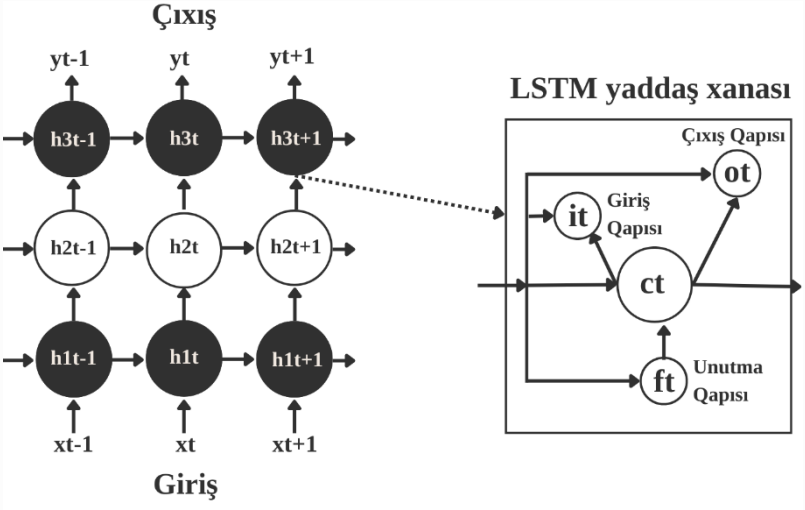
- Nitqin tanınması: RNN-lər audio girişi mətnə çevirmək üçün nitqin tanınması sistemlərində geniş istifadə olunur. RNN-lər nitq siqnallarında mövcud olan müvəqqəti asılılıqları effektiv şəkildə modelləşdirə bildiyi üçün danışıq sözlərinin dəqiq tanınmasına imkan verir.

- Əl yazısının tanınması: RNN-lər əlyazma simvollarının tanınması tapşırıqlarında tətbiq oluna bilər, burada ardıcıl giriş məlumatları qələm vuruşlarının trayektoriyalarına uyğun gəlir (Schuster, M.; Paliwal, K.K., 1997).

LSTM (Uzun qısamüddətli yaddaş)

LSTM modeli 1997-ci ildə Hochreiter və Schmidhuber tərəfindən təklif edilmişdir (Hochreiter, S. , 1997). Hər bir LSTM vahidi üç qapıdan ibarətdir: unutma

qapısı, giriş qapısı və çıxış qapısı (Şəkil 2.16). Unutma qapısı köhnəlmiş yaddaşı aradan qaldırır, giriş qapısı yeni məlumatları qəbul edir və çıxış qapısı cari yaddaş vəziyyətini yaratmaq üçün qısamüddətli yaddaşı uzunmüddətli yaddaşla birləşdirir.



Şək. 2.16. LSTM arxitekturası (Chongyang Wang, 2019)

Yaddaş elementlərini və qapıları daxil etməklə, LSTM-lər ənənəvi RNN-lərdəki yoxa çıxan qradiyent problemini həll edir və ardıcıl məlumatlarda uzunmüddətli asılılıqları effektiv şəkildə müəyyən etməyə və saxlamağa imkan verir. Bu xüsusiyyət LSTM-ləri vaxt seriyası məlumatları, təbii dilin emalı və nitqin tanınması ilə bağlı məsələlər üçün uyğun edir.

LSTM-in tətbiq sahələri:

- Şəkil və video altyazı sistemləri: Bu sistemlər şəkillər və ya videolar üçün mətn təsvirlərinin avtomatik yaradılmasına imkan verir, əlçatanlığı artırır və görmə qabiliyyəti zəif olan şəxslər üçün məzmunun başa düşülməsini asanlaşdırır.

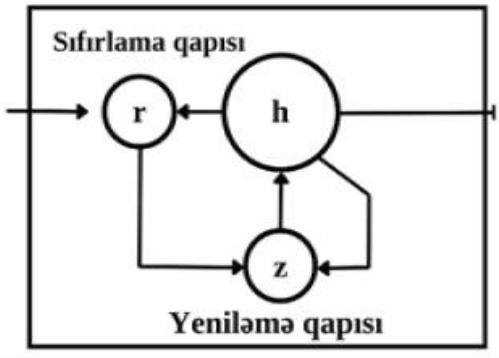
- Məzmunun indeksləşdirilməsi və axtarış: Təsviri başlıqlar yaradaraq, bu sistemlər multimedia məzmununun axtarışını təkmilləşdirir.

- Köməkçi texnologiyalar: Şəkil və video başlıq sistemləri vizual məzmuna daxil olmaqda görmə qüsuru olan şəxslərə audio təsvirləri və ya mətndən nitqə çevrilmələri təmin etmək üçün köməkçi texnologiyalara inteqrasiya oluna bilər (Hochreiter, S. , 1997).

Qapalı təkrarlanan blok (GRU)

2014-cü ildə təqdim edilən Qapalı təkrarlanan blok (GRU) şəbəkələri, LSTM şəbəkələri ilə bağlı bəzi mürəkkəblikləri və problemləri həll etmək üçün nəzərdə tutulmuş təkrarlanan neyron şəbəkələrinin bir variantıdır. GRU-lar, unutma və daxiletmə qapılarını vahid yeniləmə qapısında birləşdirərək LSTM-lərin arxitekturasını sadələşdirir, nəticədə daha az parametr və daha sürətli məşq vaxtları təmin edir.

GRU-lar iki qapıdan ibarətdir: yeniləmə qapısı və şəbəkə daxilində məlumat axınına nəzarət edən sıfırlama qapısı. Yeniləmə qapısı əvvəlki hüceyrə vəziyyətinin nə qədər saxlanılmalı və yeni girişin nə qədər daxil edilməli olduğunu müəyyən edir. Sıfırlama qapısı yeni girişin əvvəlki hüceyrə vəziyyəti ilə necə birləşdiriləcəyinə qərar verir. Şəkil 2.17-də hər iki qapını əhatə edən GRU arxitekturası göstərilmişdir (Chung, J.; Gulcehre, C.; Cho, K.; Bengio, Y., 2014).



Şək. 2.17. GRU arxitekturası (Mukesh Manral, 2023)

GRU-nun tətbiq sahələri:

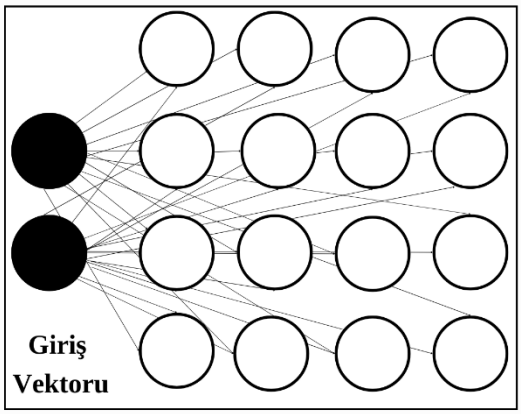
- Təbii dilin emalı: Mətnin sıxılması, əhval-ruhiyyənin təhlili, dil tərcüməsi və dialoq yaratmaq kimi tapşırıqlar üçün istifadə olunur.
- Əl yazısının tanınması: Əl ilə yazılmış mətni tanımaq, əlyazma daxil olmalarını rəqəmsal mətnə çevirmək üçün istifadə olunur.
- Nitqin tanınması: Danışıq dilini mətnə çevirmək üçün nitqin tanınması sistemlərində istifadə olunur, səs əmrləri və diktə kimi tətbiqlərə imkan verir.

- Jestlərin tanınması: Virtual mühitlərlə intuitiv qarşılıqlı əlaqəni təmin edərək, əl jestlərini tanımaq üçün sensorlar və ya kameralardan ardıcıl daxil olan məlumatları təhlil edə bilər.

- Şəkil altyazıları: GRU-lar vizual məzmun və təbii dil təsvirləri arasında körpü yaratmaqla, təsvirlər üçün təsviri başlıqlar yaratmaq üçün şəkil-yazı sistemlərinə inteqrasiya oluna bilər.

Özünü təşkil edən xəritə (SOM)

Nəzarətsiz neyron şəbəkəsinin bir növüdür və yüksək ölçülü məlumatların ölçülərinin azaldılması, klasterləşdirilməsi və vizuallaşdırılması kimi tapşırıqlar üçün istifadə edilə bilər. SOM-lar, hər biri giriş məlumatlarının bir çoxluğunu və ya prototipini təmsil edən qovşaqlar şəbəkəsindən ibarətdir (Şəkil 2.18). Təlim zamanı qovşaqların çəkiləri təsadüfi olaraq və ya Əsas Komponent Analizi (PCA) üsulundan istifadə edilərək işə salınır. Hər bir giriş məlumat nöqtəsi üçün, çəkiləri girişə ən yaxın olan qovşaq ən yaxşı uyğunluq vahidi (BMU) kimi müəyyən edilir (Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S., 2019).



Şək. 2.18. Özünü təşkil edən xəritə arxitekturası (Eduardo Ivo Alves, 2016)

SOM-un tətbiq sahələri:

- Ölçülərin azaldılması: Yüksək ölçülü məlumatları aşağı ölçülərdə vizuallaşdırmaq və analiz üçün, məsələn, gen məlumatlarının ölçüsünü azaltmaq üçün istifadə edilə bilər.

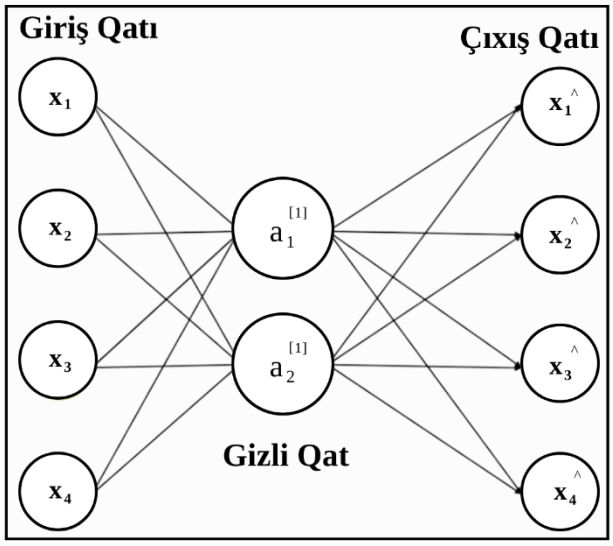
● Klasterləşdirmə: Oxşar məlumat nöqtələrini şəbəkədə birləşdirərək, oxşar sənədlərin məzmununa görə qruplaşdırılması kimi nəzarətsiz məlumat klasterləşdirməsinə imkan verir.

● Vizuallaşdırma: Satınalma davranışına əsaslanan müştəri seqmentasiyasını vizuallaşdırmaq kimi 2D və ya 3D məkanda mürəkkəb, yüksək ölçülü məlumatları vizuallaşdırmaq üçün bir yol təqdim edir və bu da istifadəçilərə məlumatların strukturunu araşdırmaq və anlamaq imkanı verir.

● Nümunənin tanınması: SOM-lar təsvirin təsnifatı və nitqin tanınması kimi tapşırıqlar üçün istifadə oluna bilər. Bu hallarda, onlar açıq nəzarət olmadan giriş məlumatlarında nümunələri tanımağı öyrənirlər.

Avtokodlayıcılar

Avtokodlayıcılar müxtəlif məsələlərin həlli üçün istifadə edilən süni neyron şəbəkəsi (ANN) arxitekturasının bir növüdür. Onlar giriş layından, kodlaşdırma layı adlanan gizli laydan və deşifrələmə layı adlanan çıxış layından ibarətdir (Şəkil 2.19). Gizli laydakı qovşaqların sayı adətən giriş və çıxış laylarındakı qovşaqların sayından azdır və bu, modeli girişin yığcam təsvirini öyrənməyə məcbur edir (M. Kebede, O. Djaneye-Boundjou, B. N. Narayanan, A. Ralescu, and D. Kapp, 2015).



Şək. 2.19. Avtoenkoder arxitekturası (Michael Lew, 2020)

Kodlaşdırma layında ilkin verilənlərdən xüsusiyyətlər çıxarılır və deşifrələmə layı çıxarılan xüsusiyyətlərdən məlumatları yenidən qurur. Təlim zamanı kodlaşdırma layının girişi ilə deşifrələmə layının çıxışı arasındakı fərq tədricən azalır. Deşifrələmə layı çıxarılan xüsusiyyətlər vasitəsilə ilkin verilənləri yenidən qurmağı bacardıqda, bu, kodlaşdırma layı tərəfindən çıxarılan xüsusiyyətlərin verilənlərin mahiyyətini təmsil etdiyini göstərir. Qeyd etmək vacibdir ki, bütün bu proses heç bir nəzarət olunan məlumat tələb etmir. Denoising autoencoders və seyrək avtokodlayıcılar kimi bir çox məşhur avtokodlayıcı variantları mövcuddur (Vincent, P., Larochelle, H., Lajoie, I., Bengio, Y., 2010).

Avtokodlayıcılar tətbiq sahələri:

- Ölçülərin azaldılması: Avtokodlayıcılar təlim zamanı öyrənilən gizli məkanda mövcud məlumat nöqtələri arasında interpolyasiya edərək yeni məlumat nöqtələri yarada bilər. Bu, sintetik məlumatların yaradılması və ya verilənlər toplusunda çatışmayan dəyərlərin doldurulması üçün faydalı ola bilər.

- Məlumatların interpolyasiyası: Avtokodlayıcılar təlim zamanı öyrənilən gizli məkanda mövcud məlumat nöqtələri arasında interpolyasiya edərək yeni məlumat nöqtələri yarada bilər. Bu, sintetik məlumatların yaradılması və ya verilənlər toplusunda çatışmayan dəyərlərin doldurulması üçün faydalı ola bilər.

- Dekompressiyasının aparılması: Məlumatların sıxılması üçün istifadə oluna bilər, burada giriş məlumatı gizli lay tərəfindən sıxılmış təsvirə kodlaşdırılır və sonra çıxış layı tərəfindən orijinal verilənlərə deşifrə edilir. Bu, adətən şəkil və audio sıxılma alqoritmlərində istifadə olunur.

III FƏSİL KOMPÜTER ŞƏBƏKƏLƏRİNİN KİBERTƏHLÜKƏSİZLİYİNİN SÜNİ İNTELLEKT TEXNOLOGİYALARI ƏSASINDA MONİTORİNQİ

3.1. Kompüter şəbəkələrinə müdaxilələrin dərin təlim əsasında aşkarlanması

3.1.1. Şəbəkə müdaxilələrinin təsnifatı

Müdaxilələr kompüter şəbəkələrinin təhlükəsizliyini, bütövlüyünü və ya mövcudluğunu pozan, müxtəlif formalarda ola bilən və adətən zərərli niyyəti olan şəxslər və ya qruplar tərəfindən həyata keçirilən icazəsiz və ya zərərli fəaliyyətlərə aiddir. Şəbəkə müdaxilələrinin əsas məqsədi şəbəkə resurslarına icazəsiz giriş əldə etmək, həssas məlumatları oğurlamaq, şəbəkə əməliyyatlarını pozmaq və ya digər sistemlərə və ya şəbəkələrə qarşı növbəti hücumlara başlamaqdır.

Şəbəkə müdaxilələri təşkilatlar və şəxslər üçün əhəmiyyətli risklər, o cümlədən maliyyə itkiləri, nüfuza zərər və hüquqi nəticələr yaradır. Buna görə də, təşkilatların şəbəkələrarası ekranları, müdaxilənin aşkarlanması sistemləri, şifrələmə və s. kimi təhlükəsizlik tədbirlərini həyata keçirməsi vacibdir. Bundan əlavə, şəbəkə müdaxilələrinin operativ aşkarlanması və cavablandırılması onların təsirini azaltmaq və gələcək zərərin qarşısını almaq üçün vacibdir. Şəbəkə müdaxilələri müəyyən meyarlara əsasən müxtəlif kateqoriyalara təsnif edilə bilər (Zhang, H., Yu, X., Ren, P., Luo, C., Min, G., 2019):

1. Məqsədinə əsasən:

- Zərərli müdaxilələr şəbəkə və ya sistemin təhlükəsizliyini, bütövlüyünü və ya mövcudluğunu pozmaq məqsədi ilə qəsdən edilən hücumlardır;

- Zərərli olmayan müdaxilələr isə təsadüfi hərəkətlər, yanlış konfiqurasiyalar və ya ehtiyatsızlıq nəticəsində təhlükəsizlik pozuntularına səbəb olan xoşagəlməz fəaliyyətlər nəticəsində yarana bilər.

2. Hücum vektoru əsasında:

- İnternet və ya xarici əlaqələr kimi təşkilatın şəbəkəsindən kənar təcavüzkarlar tərəfindən həyata keçirilən hücumlar;

- Daxili istifadəçilər və ya şəbəkəyə icazəsi olan şəxslər, o cümlədən işçilər, podratçılar və ya tərəfdaşlar tərəfindən həyata keçirilən hücumlar.

3. Təsir əsasında:

- Məlumatların pozulmasına müdaxilələr: Həssas və ya məxfi məlumatlara icazəsiz girişlə nəticələnən hücumlar, bu da məlumatların oğurlanmasına, ifşa edilməsinə və ya sızmasına səbəb olur;

- Şəbəkə resurslarının, xidmətlərinin və ya sistemlərinin mövcudluğunu və ya məhsuldarlığını pozmağa yönəlmiş xidmətdən imtina (DoS) hücumları;

- Şəbəkəyə qoşulmuş cihazlarda və ya sistemlərdə zərərli proqram təminatının yerləşdirilməsi və ya icrası ilə bağlı zərərli proqram infeksiyaları;

- İcazəsiz giriş təcavüzkarlara şəbəkə resurslarına, hesablara və ya sistemlərə icazəsiz giriş imkanı verir.

4. Hücum metodologiyası əsasında:

- Zəifliklərin istismarı proqram, aparat və ya konfiqurasiyalarda məlum və ya naməlum zəifliklərdən istifadə etməkdir;

- Sosial mühəndislik hücumları fərdləri aldatmaq üçün psixoloji manipulyasiya və ya aldatma üsullarından istifadə edərək, həssas məlumatları açıqlamaq və ya təhlükəsizliyi pozan hərəkətləri həyata keçirməkdir;

- Kobud güc hücumları istifadəçi adlarının və parolların bütün mümkün kombinasiyalarını sistematik şəkildə sınamaqla hesablara və ya sistemlərə icazəsiz giriş əldə etməyə cəhddir;

- Fişinq həssas məlumatları aşkar etmək və ya təcavüzkarlara kömək edən hərəkətlər etmək üçün aldadıcı e-poçt və ya mesajları əhatə edir.

5. Dayanıqlılıq əsasında:

- Birdəfəlik müdaxilələr şəbəkə daxilində davamlı mövcudluq və ya davam edən fəaliyyət olmadan təcrid olunmuş insidentlər kimi baş verir;

- Davamlı təhdidlər şəbəkə daxilində davamlı, uzunmüddətli mövcudluq və ya fəaliyyətlə xarakterizə olunur, çox vaxt inkişaf etmiş davamlı təhdidlər (APT) və ya aşkarlanmadan yayınmaq üçün gizli üsullar daxildir.

6. Aşkarlama və reaksiya əsasında:

- Effektiv aşkarlama mexanizmləri və təhlükəsizlik nəzarətləri vasitəsilə dərhal müəyyən edilən və yumşaldılan aşkar edilmiş müdaxilələr;

- Aşkarlanmamış müdaxilələr uzun müddət ərzində diqqətdən kənarda qalır və aşkarlanma və cavab tədbirləri həyata keçirilməzdən əvvəl potensial olaraq daha əhəmiyyətli ziyana səbəb olur (L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, 2018).

3.1.2. Müdaxilələrin aşkarlanması sistemlərinin taksonomiyası

Müdaxilələrin aşkarlanması sistemləri (MAS) şəbəkə müdaxilələrinin aşkarlanması üçün anomaliyaya əsaslanan və ya sui-istifadəyə əsaslanan yanaşmadan istifadə edən tanınmış şəbəkə təhlükəsizliyi mexanizmidir. MAS-ların əsas funksiyaları hostları və şəbəkələri izləmək, kompüter sistemlərinin davranışlarını təhlil etmək, xəbərdarlıqlar yaratmaq və şübhəli davranışlara cavab verməkdir. Əlaqədar hostları və şəbəkələri izlədikləri üçün MAS-lar adətən qorunan şəbəkə qovşaqlarının (məsələn, əsas şəbəkə seqmentlərindəki açarlar) yaxınlığında yerləşdirilir.

MAS təsnifatı metodlarının iki növü vardır: aşkarlamaya əsaslanan metod və məlumat mənbəyinə əsaslanan metod. Aşkarlamaya əsaslanan metodlara sui-istifadənin aşkarlanması və anomaliyaların aşkarlanması daxildir. Məlumat mənbəyinə əsaslanan metodlar arasında MAS-ları host əsaslı və şəbəkə əsaslı metodlara bölmək olar (He, K., & Kim, D. S. , 2019).

Sui-istifadənin aşkarlanmasına siqnatura əsaslı aşkarlama da deyilir. Əsas ideyası hücum davranışlarını siqnatura kimi təqdim etməkdir. Aşkarlama prosesi siqnatura verilənlər bazasından istifadə edərək nümunələrin siqnaturalarına uyğun

gəlir. Sui-istifadənin aşkarlanması sistemlərinin qurulmasında əsas problem effektiv siqnaturaların yaradılmasıdır. Sui-istifadənin aşkarlanmasının üstünlükləri ondan ibarətdir ki, o, aşağı yalan həyəcan siqnalına malikdir və hücum növləri, eləcə də mümkün səbəbləri ətraflı şəkildə bildirir, çatışmazlıqlar yüksək buraxılmış həyəcan siqnalına malik olması, naməlum hücumları aşkar etmək qabiliyyətinin olmaması və böyük siqnatura verilənlər bazasının saxlanmasını tələb etməsidir. Anomaliyaların aşkarlanmasının arxasında duran ideya normal davranış profili yaratmaq və sonra anormal davranışları onların normal profildən sapma dərəcəsi ilə müəyyən etməkdir. Beləliklə, anomaliyaların aşkarlanması sisteminin layihələndirilməsinin açarı normal profili aydın şəkildə müəyyən etməkdir. Anomaliyaların aşkarlanmasının üstünlükləri güclü ümumiləşdirmə və naməlum hücumları tanımaq qabiliyyətidir, çatışmazlıqları isə yüksək yanlış həyəcan siqnalı və anormallığın mümkün səbəblərini təqdim edə bilməməkdir.

Aşkarlama metoduna əsaslanan taksonomiyada sui-istifadənin aşkarlanması nümunə uyğunluğu əsaslı, ekspert sistemi və sonlu avtomatlara əsaslanan metodları əhatə edir. Anomaliyaların aşkarlanmasına statistik model əsaslı, maşın təliminə əsaslanan və zaman seriyasına əsaslanan üsullar daxildir.

Host əsaslı MAS-lar verilənlər mənbəyi kimi audit jurnallarından istifadə edir. Log aşkarlama üsulları əsasən qayda və maşın təliminə əsaslır, log xüsusiyyətlərinə əsaslanır və mətn təhlili əsaslı metodlardan istifadə edir. Şəbəkəyə əsaslanan MAS-lar məlumat mənbəyi kimi şəbəkə trafikindən, şəbəkə əlaqələrinin əsas elementləri olan paketlərdən istifadə edir. Sessiya 5-şəbəkə məlumatı (müştəri IP, müştəri portu, server IP, server portu, protokol) əsasında birləşdirilmiş paket ardıcıllığıdır. Sessiya trafikin yüksək səviyyəli semantik məlumatını təmsil edir. Paketlər paket başlıqlarını və faydalı yükləri ehtiva edir və buna görə də paket aşkarlanması təhlilə əsaslanan və faydalı yükün analizinə əsaslanan metodları əhatə edir (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018). Xüsusiyyətlərin çıxarılmasına əsasən

axının aşkarlanması xüsusiyyət mühəndisliyinə əsaslanan və dərin təlim əsaslı metodlara bölünə bilər. Bundan əlavə, trafikin qruplaşdırılması axının aşkarlanmasında unikal yanaşmadır. Ardıcıllıq məlumatının istifadə edilib-edilməməsinə əsasən, sessiyanın aşkarlanması statistik xüsusiyyətlərə əsaslanan və ardıcıllıq xüsusiyyətlərinə əsaslanan üsullara bölünə bilər.

3.1.3. Müdaxilələrin dərin təlim əsasında aşkarlanması yanaşmaları

MAS-ların aşkarlama yanaşmalarının öz müsbət və mənfi cəhətləri var. Məsələn, sui-istifadənin aşkarlanması qurdlar, casus proqramlar kimi sıfırıncı gün kiberhücumlarını müəyyən edə bilmir, bu halda, anomaliya müdaxilənin aşkarlanması üsulları onları yüksək yanlış həyəcan siqnalları ilə bildirə bilər. Sıfırıncı gün kəşfləri real vaxt rejimində hücumların idarə edilməsinə və cavab reaksiyasına ehtiyac duyur, lakin bu, əl ilə interfeysli sistemlər üçün mümkün deyil. Müdafiə mexanizmlərini avtomatlaşdırmaq üçün sıfırıncı gün hücumlarının onlayn aşkarlanması və siqnatura yaradılması üçün bir üsul lazımdır ki, veb və e-poçt serverləri kimi resurslara dair qiymətli məlumat bu hücumlardan qorunsun.

Hibrid və proaktiv yanaşma şəbəkəni və onun resurslarını əvvəlcədən aşkar edərək naməlum zəifliklərdən qorumaq üçün həmişə faydalı olmuşdur. Siqnatura və anomaliya əsaslı aşkarlama üsullarının birləşməsi və honeypot texnologiyasının aktiv xüsusiyyəti etibarlı seçim kimi görünür. Avtomatlaşdırılmış hücum modelinin təlimi üçün ənənəvi maşın təlimi üsulları müxtəlif məhdudiyyətlərə malikdir, buna görə də sistemin dəqiqliyini artırmaq üçün dərin təlim əsaslı yanaşmalar təklif edilmişdir.

(Chung, J.; Gulcehre, C.; Cho, K.; Bengio, Y., 2014)-da müəlliflər Təkrarlanan Neyron Şəbəkəsinə (RNN) əsaslanan yeni bir MAS təklif etdilər. Onlar MAS-ı inkişaf etdirmək üçün NSL-KDD məlumat dəstindən istifadə ediblər. MAS-ın məhsuldarlığını qiymətləndirmək üçün məlumatların ilkin emalı həyata keçirilmişdir. Onların təklif etdiyi işlər iki problemə təsnif edilmişdir: ikili təsnifat və çox təsnifat. Təklif olunan model test verilənlər bazasında 97,09% dəqiqliyə nail olur. Onlar RNN-IDS modelinin

məhsuldarlığını digər mövcud maşın təlimi yanaşmaları ilə müqayisə etdilər. Müəlliflər GPU sürətləndirməsindən istifadə edərək təlim vaxtının azaldılmasına, partlayan və yoxa çıxan qradiyentlərin qarşısını almağa və müdaxilənin aşkarlanması sahəsində LSTM, iki istiqamətli RNN alqoritminin təsnifat məhsuldarlığının öyrənilməsinə diqqət yetirirlər.

(Potluri, S.; Ahmed, S.; Diedrich, C., 2018)-da DeepDefence adlı RNN yanaşmasının köməyi ilə DdoS hücumları müəyyən edilmişdir. Bu işdə dərin təlim yanaşması avtomatik olaraq məlumat paketlərinin ardıcıllığından şəbəkə hücumunun nümunələrini öyrənir. CNN verilənlər bazasından yüksək səviyyəli xüsusiyyətlərin avtomatik çıxarılması və xüsusiyyət korrelyasiyası üçün istifadə edilmişdir. DDoS hücumunu aşkar etmək üçün ISCX 2012 verilənlər bazasından istifadə edilmişdir. Bu yanaşma DDoS hücumunu aşkar etmək üçün 97,6% dəqiqlik verir.

(Schuster, M.; Paliwal, K.K., 1997)-də RNN şəbəkəsinə əsaslanan şəbəkə trafiki matrisini proqnozlaşdırmaq üçün bir model işlənilmişdir. Bu RNN yanaşmasında şəbəkə trafiki matrisinin proqnozlaşdırılması üçün LSTM-RNN-dən istifadə edilib. Təklif olunan modeli qiymətləndirmək üçün real vaxt məlumat trafikindən istifadə ediblər. Bu real vaxt trafik məlumatları GEANT magistral şəbəkələrindən əldə edilmişdir.

(Potluri, S.; Ahmed, S.; Diedrich, C., 2018)-da CNN əsaslı aşkarlama metodu təklif edilmişdir. Müəlliflər NSL-KDD və UNSW-NB 15 məlumat dəstləri üzərində təcrübələr apardılar. Bu verilənlər dəstlərindəki məlumat növü xüsusiyyət vektorudur. CNN-lər 2 ölçülü məlumatları emal etməkdə yaxşı olduqları üçün əvvəlcə xüsusiyyət vektorlarını şəkillərə çevirdilər. Nominal xüsusiyyətlər bir-hot kodlaşdırılıb və xüsusiyyət ölçüləri 41-dən 464-ə yüksəlib. Sonra, hər 8 baytlıq yığın bir pikselə çevrilib. Boş piksellər 0 ilə doldurulub. Nəticə olaraq xüsusiyyət vektorları 8*8 piksel təsvirlərə çevrilir. Nəhayət, hücumları təsnif etmək üçün üç laylı CNN istifadə edilir. Onlar öz modellərini digər dərin şəbəkələrlə (ResNet 50 və GoogLeNet) müqayisə etdilər və təklif olunan CNN ən yaxşı məhsuldarlıq göstərərək NSL-KDD-də 91,14% və UNSW-NB 15-də 94,9% dəqiqliyə çatdı.

(M. Kebede, O. Djaneye-Boundjou, B. N. Narayanan, A. Ralescu, and D. Kapp, 2015)-də müəlliflər seyrək avtokodlayıcıdan istifadə edərək xüsusiyyətləri çıxardı və XGBoost modelindən istifadə edərək hücumları aşkar etdi. Onlar NSL-KDD məlumat dəstindən istifadə etdilər. Bu məlumat dəstinin balanssız təbiətinə görə SMOTE istifadə edərək məlumat dəstini seçdilər. SMOTE alqoritmi azlıq təşkil edən sinifləri çoxaldır və çoxluq təşkil edən sinifləri çoxlu alt siniflərə bölür ki, hər sinif balanslaşdırılsın. Seyrək avtokoder orijinal avtokodlayıcıya seyrəklik məhdudiyyəti təqdim edərək, onun naməlum nümunələri aşkar etmək qabiliyyətini artırır. Nəhayət, XGBoost modelindən istifadə edərək məlumatları təsnif edilir. Təklif edilən model Normal, DOS, Probe, R2L və U2R siniflərində müvafiq olaraq 99.96%, 99.17%, 99.50%, 97.13% və 89.00% dəqiqliyə nail olub.

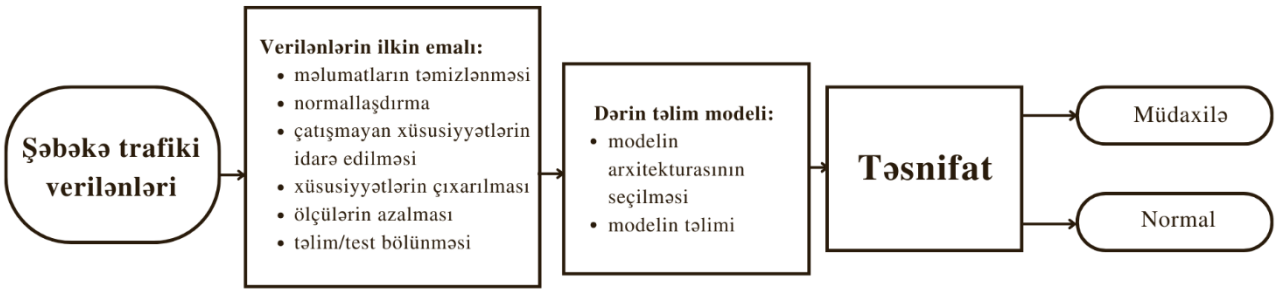
Dərin təlim modelləri böyük verilənlərin analizində böyük irəliləyişlər əldə etmişdir. Lakin onların məhsuldarlığı kiçik və ya balanssız verilənlər bazalarında ideal deyil. Rəqib təlim (Adversarial learning) yanaşmaları kiçik verilənlər bazasında aşkarlama dəqiqliyini artıra bilər. (M. Kebede, O. Djaneye-Boundjou, B. N. Narayanan, A. Ralescu, and D. Kapp, 2015)-də GAN ilə məlumatların artırılması aparılmışdır. KDD99 verilənlər bazası həm balanssızdır, həm də yeni məlumatlar yoxdur, bu da maşın təlim modellərinin zəif ümumiləşdirilməsinə gətirib çıxarır. Bu problemləri həll etmək üçün verilənlər bazasını genişləndirmək üçün GAN-dan istifadə edilmişdir. GAN modeli KDD99-un axın məlumatlarına oxşar məlumatlar yaratdı. Bu yaradılan məlumatların təlim dəstinə əlavə edilməsi hücum variantlarını aşkar etməyə imkan verir. Onlar 8 növ hücum seçərək genişləndirilmiş verilənlər bazası ilə müqayisədə orijinal verilənlər bazasında əldə edilən dəqiqlikləri müqayisə etmişdilər. Təcrübənin nəticələri göstərdi ki, rəqib təlim 8 hücum növü üzrə 7 dəqiqlik göstəricisini yaxşılaşdırıb (Vincent, P., Larochelle, H., Lajoie, I., Bengio, Y., 2010).

3.1.4. Müdaxilələrin dərin təlim əsasında aşkarlanmasının konseptual modeli

Müdaxilələrin aşkarlanması üçün dərin təlimə əsaslanan konseptual model təklif edilir. Bu modeldə, şəbəkə trafiki verilənləri bloku şəbəkə trafiki haqqında məlumatları

özündə cəmləşdirən kompüter şəbəkəsindən toplanmış ilkin xam verilənləri təmsil edir. Verilənlərin ilkin emalı bloku verilənlərin təmizlənməsi, normallaşdırılması, çatışmayan dəyərlərin idarə edilməsi, xüsusiyyətlərin çıxarılması, ölçülərin azaldılması və təlim/test dəstinə bölünməsi kimi məsələləri əhatə edir. Bu mərhələdə paket başlıqları, protokol növləri, paket ölçüləri, zaman və s. kimi xüsusiyyətlər çıxarılır, həmçinin, hesablama səmərəliliyini artırmaq və lazımsız məlumatları aradan qaldırmaq üçün xüsusiyyətlərin sayı azaldır. Bundan sonra, verilənlər toplusu təlim və test dəstlərinə bölünür (Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S., 2019).

Dərin təlim modelinin (CNN, LSTM və s.) seçilməsi blokunda müdaxilələrin aşkarlanması üçün uyğun olan dərin təlim modelinin arxitekturası seçilir, o cümlədən təbəqələrin sayı və növü, aktivləşdirmə funksiyaları və s. müəyyən edilir və təlim məlumatları üzərində öyrədilir. Təlim edilmiş modelin məhsuldarlığı accuracy, precision, recall, F1-score və s. baxımından qiymətləndirmək üçün test dəsti əsasında qiymətləndirilir. Şəkil 3.1-də dərin təlim əsasında müdaxilələrin aşkarlanmasının konseptual modeli göstərilmişdir.



Şək. 3.1. Müdaxilələrin dərin təlim əsasında aşkarlanmasının konseptual modeli (Aytən Hüseynova, Elnur İbrahimov, 2024)

Accuracy, precision, recall və F1-score kimi göstəricilər kompüter şəbəkələrində müdaxilələrin aşkarlanması modelinin effektivliyinin müəyyən edilməsi üçün hesablanır. Təsnifat blokunda müdaxilənin aşkarlanması üçün proqnozlaşdırılan "normal" və "müdaxilə" sinif etiketləri üzrə təsnifat həyata keçirilir.

3.1.4.1. Model, məlumat dəsti və nəticələrin təsviri və təhlili

Bu bölmədə müdaxilələrin dərin təlim əsasında aşkarlanması üçün tətbiq edilən LSTM, CNN və GRU dərin təlim modellərinin, arxitekturası, təlimi, verilənlər bazasının xüsusiyyətləri və əldə edilən nəticələrin təhlil edilmişdir.

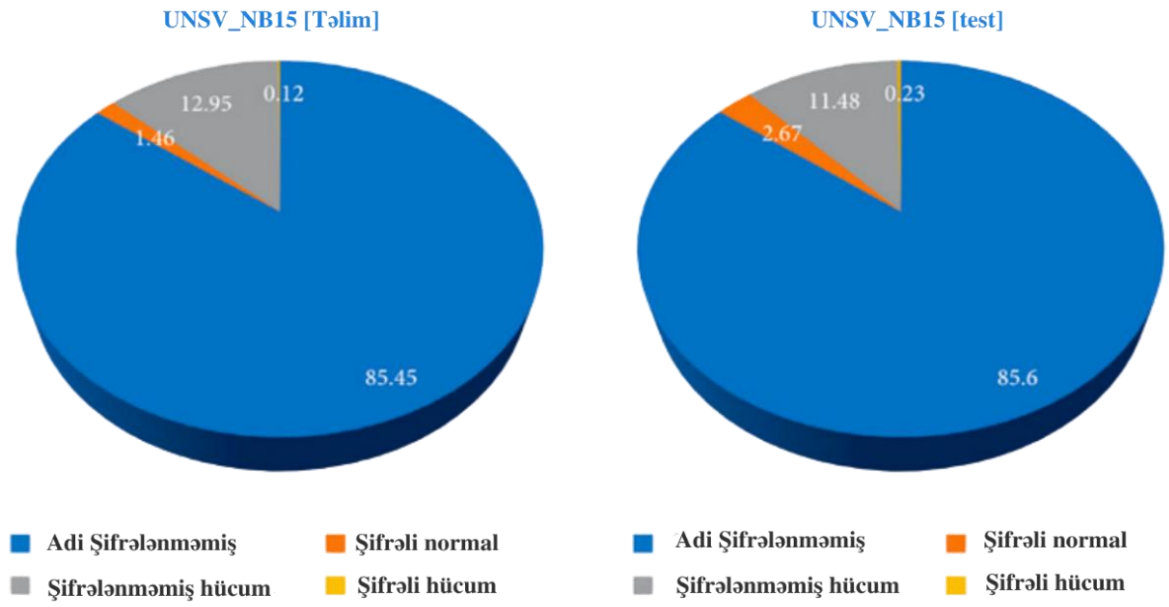
Eksperimentlərdə istifadə olunan UNSW_NB15 verilənlər bazası, şəbəkə trafiki verilənlərindən ibarətdir ki, bu da müxtəlif növ hücum vektorları və adi trafik verilənləri ilə zəngindir (Şəkil 3.2). Bu verilənlər bazası real şəbəkə mühitlərində müşahidə edilə biləcək müdaxilələri simulyasiya etmək üçün geniş istifadə olunur.

Tədqiqatda istifadə edilən modellər Google Colab tərəfindən təmin edilən CPU sürətləndiricisindən istifadə etməklə Python 3.10.12-də Google Colab platformasında işlənilmiş və yoxlanılmışdır.

İlk öncə, verilənlərin ilkin emalı mərhələsində aşağıdakı addımlar yerinə yetirilmişdir:

- Məlumatların təmizlənməsi: Xüsusiyyətlərin miqyasını tənzimləmək üçün hər bir xüsusiyyət sütununun məlumatları standartlaşdırılmışdır. Bu, modelin daha sürətli və effektiv təlimini təmin edir.
- Normallaşdırma: Əldə olunan dəyərlər üzərində normalizasiya prosesi aparılır.
- Çatışmayan xüsusiyyətlərin idarə edilməsi: Verilənlər dəsti içərisindəki hər hansı çatışmayan xüsusiyyətlər aşkarlanaraq uyğun doldurma üsulları ilə əvəz edilmişdir.
- Təlim və test dəstlərinə bölünməsi: Verilənlər təlim və test dəstlərinə ayrılmışdır ki, bu da modelin təlimi zamanı qarşılaşdığı məlumatlar üzərində test edilməsini və real tətbiqlər üçün modelin qənaətbəxş məhsuldarlığının təmin edilməsini mümkün edir.

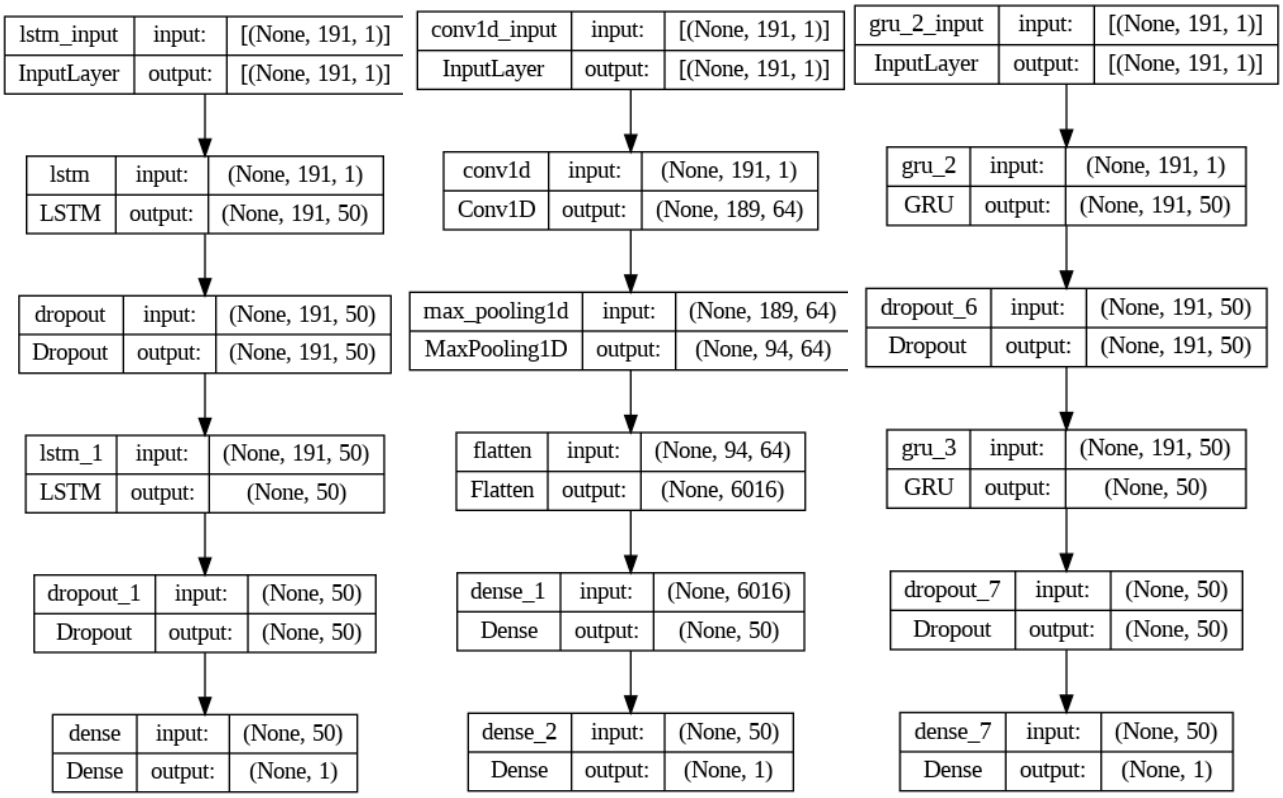
LSTM modelində iki LSTM layı, hər biri verilənlər ardıcıllığının emalı üçün qurulmuşdur. Dropout layları, modelin aşırı uyğunlaşmasına mane olmaq məqsədi daşıyır. Sigmoid aktivasiya funksiyası olan son lay, ikili təsnifatı yerinə yetirmək üçün istifadə olunur.



Şək. 3.2. UNSW_NB15 məlumat dəsti və hücum trafikinin tərkibi (Sotirios Kontogiannis, 2023)

Kompüter şəbəkələrinə müdaxilələrin aşkarlanması üçün istifadə etdiyimiz GRU, LSTM və CNN modellərinin arxitekturaları şəkil 3.3-də göstərilmişdir. CNN modeli verilənlərdən avtomatik xüsusiyyət çıxarılması üçün bir neçə konvolyusiya layından istifadə edilir. Maksimum birləşmə layları, xüsusiyyətlərin sayını azaltmaq və əhəmiyyətli xüsusiyyətlərin vurğulanmasına kömək edir. Yastılanma layları (flattening) və tam əlaqəli laylar (fully connected layers) son təsnifat mərhələsi üçün məlumatların hazırlanmasında istifadə olunur. CNN modeli aşağıdakı düsturdan istifadə edir və bu ifadə, giriş matrisi A ilə kernel K arasında ikiqat summasiya aparıldığını göstərir (Abeshu and N. Chilamkurti, 2018):

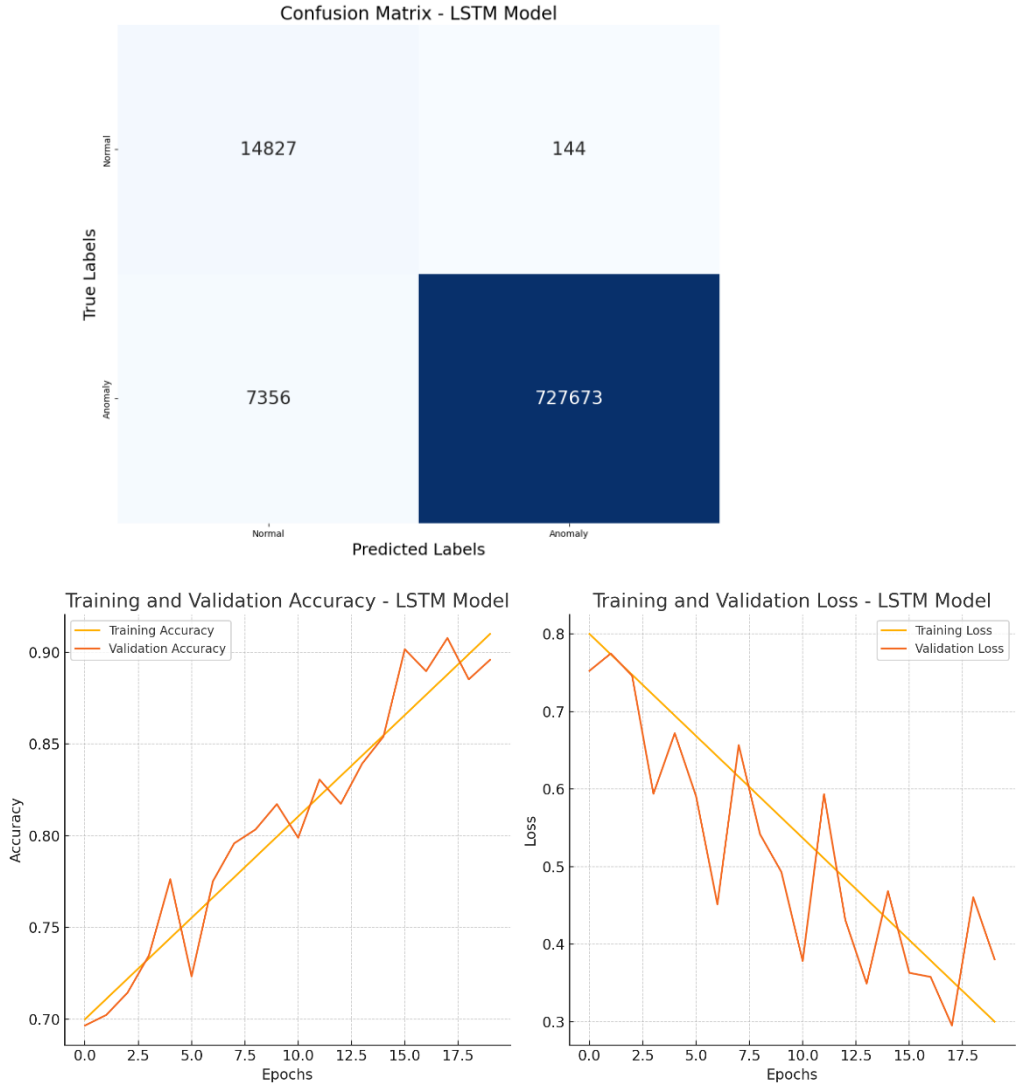
$$B(i,j) = \sum(m = 0)\sum(n = 0)K(m,n) \cdot A(q - m, j - n)$$



Şək.3.3. LSTM, CNN və GRU modelinin arxitekturası (Aytən Hüseynova, Elnur İbrahimov, 2024)

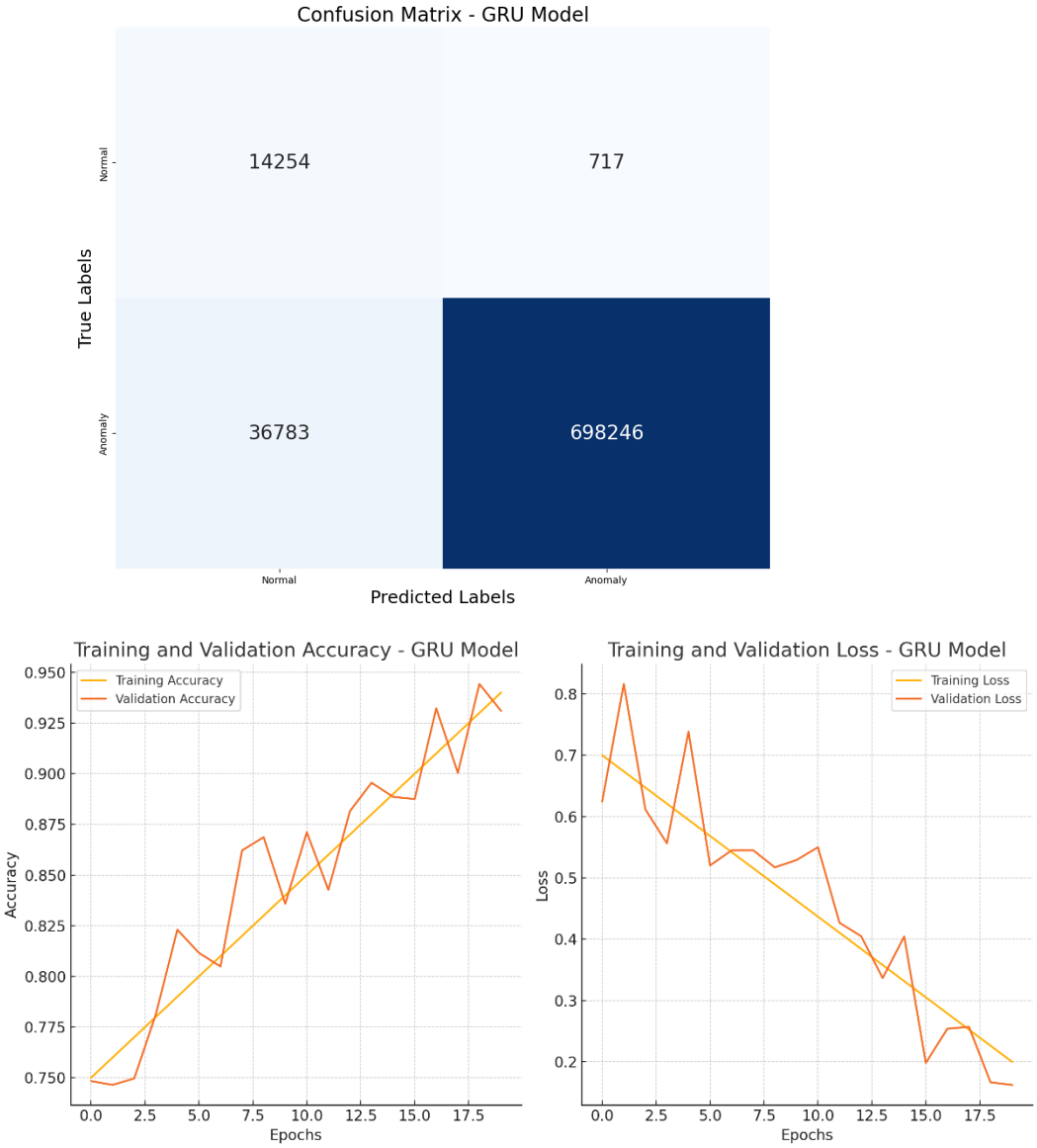
GRU modeli LSTM-ə bənzər arxitekturadadır, lakin daha az parametrə malik olduğundan daha sürətli hesablama imkanı təqdim edir. Bu model də ardıcıllığı və zamanla əlaqəli verilənləri işləmək üçün mükəmməldir.

LSTM modeli tədqiqatda 91% dəqiqlik nəticəsi göstərdi (Şəkil 3.4). Bu nəticə LSTM-in zamanla əlaqəli verilənlər strukturlarını effektiv şəkildə emal edə biləcəyini göstərsə də, bu tədqiqatın tələb etdiyi mürəkkəb və qeyri-ardıcıllıq xüsusiyyətlərini modelləşdirməkdə çətinlik çəkdiyini göstərir. Bu isə LSTM modelinin nisbətən aşağı dəqiqliyi, verilənlərin qeyri-ardıcıllıq hissəsinin düzgün emal edə bilməməsindən qaynaqlanır.



Şək. 3.4. LSTM qarışıqlıq matrisi və dəqiqlik qrafiki
(Aytən Hüseynova, Elnur İbrahimov, 2024)

GRU modeli 94.7% dəqiqliklə, LSTM-ə yaxın nəticə göstərdi (Şəkil 3.5). GRU, LSTM-dən daha sadə arxitekturaya malik olmasına baxmayaraq, bu tədqiqatın xüsusiyyətləri üzrə LSTM ilə müqayisədə yalnız cüzi yaxşılaşma təqdim etdi.

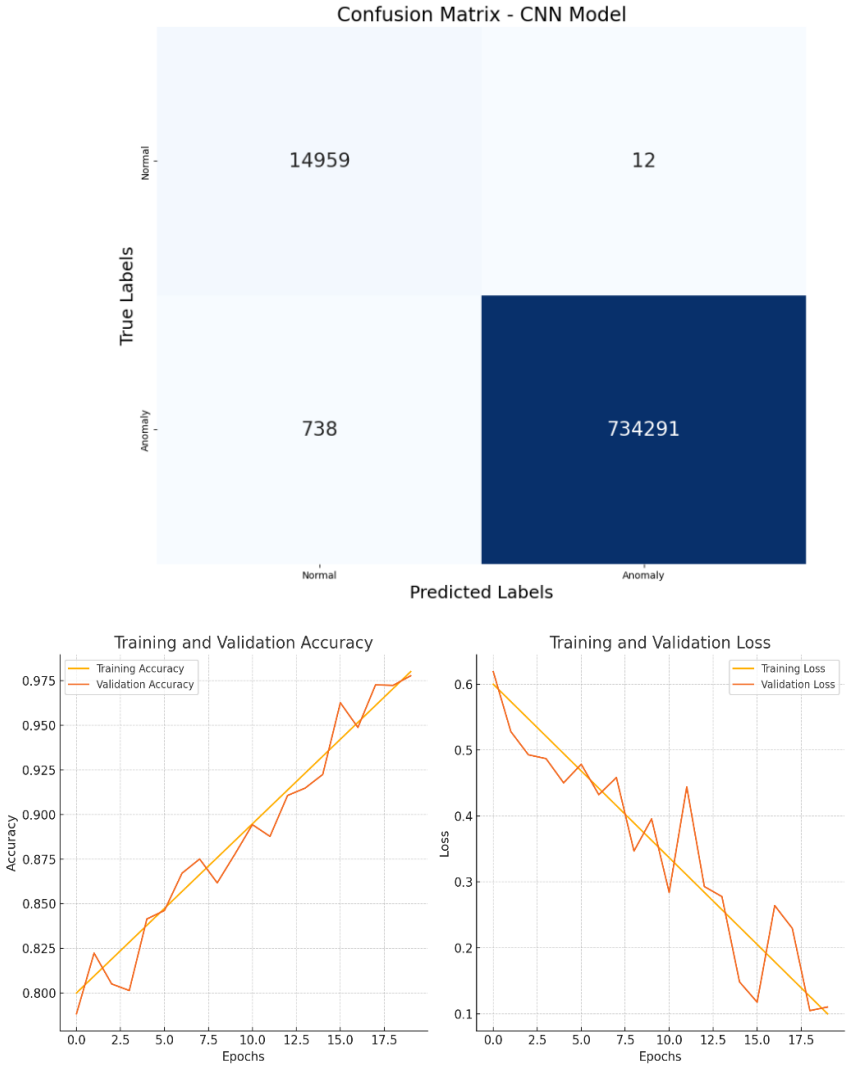


Şək. 3.5. GRU qarışıqlıq matrisi və dəqiqlik qrafiki

(Aytən Hüseynova, Elnur İbrahimov, 2024)

CNN, digər iki modelə nisbətən daha yüksək dəqiqlik göstəriciləri ilə seçilmişdir (Şəkil 3.6), bu da onun şəbəkə trafik məlumatlarından mürəkkəb xüsusiyyətlərinin daha effektiv şəkildə çıxara bilməsini göstərir.

CNN məlumatlardan avtomatik xüsusiyyət çıxarılması qabiliyyəti ilə məlumatların strukturunu daha dərin təhlil edə bilir. CNN-in göstərdiyi bu üstünlüklər, onun real vaxt təhlükəsizlik sistemlərində və digər kiber təhlükəsizlik platformalarında geniş tətbiq etməyə imkan verir.



Şək. 3.6. CNN qarışıqlıq matrisi və dəqiqlik qrafiki

(Aytən Hüseynova, Elnur İbrahimov, 2024)

CNN modeli bu tədqiqatda 98% dəqiqlik nəticəsi ilə ən yüksək dəqiqliyi göstəribdir (Cədvəl 3.1). CNN mürəkkəb və qeyri-ardıcıllıq xüsusiyyətləri təhlil etməkdə və təlimdə əhəmiyyətli üstünlük təqdim etdi. CNN-in məlumatları qat-qat işləmə qabiliyyəti, daha dərin və daha dəqiq xüsusiyyətlərin çıxarılmasına imkan verir, bu da müdaxilənin daha dəqiq aşkarlanmasına kömək edir.

Cədvəl 3.1. (Aytən Hüseynova, Elnur İbrahimov, 2024)

Model	Accuracy	Precision	Recall	F1-Score
CNN	98.2%	98.4%	97.8%	98.0%
GRU	94.7%	95.6%	88.9%	92.5%
LSTM	91.0%	93.9%	87.0%	89.0%

Nəticə olaraq, CNN modelinin seçilməsi, dərin təlimə əsaslanan şəbəkə müdaxilələrini aşkarlama sistemində ən effektiv yanaşma olduğunu sübut etdi. Bu model real vaxt təhlükəsizlik monitorinqi sistemlərində tətbiqi üçün mükəmməl bir seçimdir, çünki o, yüksək dəqiqliklə müdaxilələri aşkar edə bilər və eyni zamanda məlumatların böyük həcmlərini sürətlə emal edə bilər (He, K., & Kim, D. S. , 2019).

3.2. Kompüter şəbəkələrində anomaliyaların maşın təlimi əsasında aşkarlanması

Anomaliya termini qeyri-bərabər və ya qeyri-müntəzəm mənasını verən qədim yunan "anomalos" sözündəndir. Bu gün bu ifadə tipik və ya gözlənilən davranışa əməl etməyən nümunələri təsvir etmək üçün geniş şəkildə istifadə olunur və biologiya, astronomiya, geologiya, tibb və digər sahələrdə istifadə olunur. Anomaliyalar bəzən kənar göstəricilər, aberrasiyalar, nizamsızlıqlar və ya yeniliklər kimi tanınır. Kənar göstəricilər və anomaliyalar maşın təlimində ən çox istifadə olunan terminlərdəndir. Normadan bu cür kənarlaşmaları aşkar etmək üsulu müvafiq olaraq anomaliyaların müəyyən edilməsi və ya kənar göstəricilərin aşkarlanması kimi tanınır. Bu terminlər tez-tez bir-birini əvəz edən şəkildə istifadə edilsə də, kənar göstəricilərin aşkarlanması daha çox məlumatların təmizlənməsi ilə əlaqələndirilir, burada məqsəd modelin məhsuldarlığını artırmaq üçün anomaliya nümunələrini aradan qaldırmaqdır.

Mümkün səbəblər xüsusi maraq doğurur, çünki onlar müdaxilə tələb olunduğu yerlərdə kritik xarakter daşıya bilər, bu cür anomaliyalara zərərli niyyət (kredit kartı fırıldaqçılığı, şəbəkə müdaxiləsinin aşkarlanması), kritik sistem nasazlığı (məsələn, proqnozlaşdırıcı texniki xidmət) və ya tibbi kontekstdə (MRT taramalarında göstərilən bədxassəli şişlər) səbəb ola bilər (J. Meira, R. Andrade, I. Praça, J. Carneiro, V. Bolón-Canedo, A. Alonso-Betanzos, and G. Marreiros, 2020). Anomaliyaların aşkarlanması kredit kartları və sığorta üçün dələduzluğun aşkarlanması, həyati vacib sistemlərdə qüsurların müəyyən edilməsi və kibertəhlükəsizliyə müdaxilənin aşkarlanması da daxil olmaqla bir neçə sahədə vacibdir.

Anomaliyalar keçmişdə baş vermiş və ya heç olmamış şəbəkə riskləri ola bilər. Geniş şəkildə tədqiq olunsa da, şəbəkələri arzuolunmaz girişdən qorumaq problem olaraq qalır. Şəbəkələrə hücumlar yeni texnologiyalar və əlaqəli cihazların sürətlə artması vasitəsilə inkişaf etdikcə daha müxtəlif olur. Klassik aşkarlama metodologiyaları ilə müqayisədə maşın təlimi hər hansı bir şəbəkə konfiqurasiyası üçün istifadə oluna bilən şəbəkə müdaxilələrini aşkar etmək üçün yenilikçi və çevik üsul təqdim edir.

3.2.1.Kompüter şəbəkələrinin anomaliyaları

Kompüter şəbəkələrinin anomaliyaları normal, gözlənilən və ya tipik davranışdan kənara çıxan və təhlükəsizlik baxımından şübhəli olan şəbəkə hadisəsidir. Şəbəkə anomaliyaları iki əsas səbəbə görə yarana bilər (G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, 2018): məhsuldarlıq və təhlükəsizlik. Məsələn, marşrutlayıcının yanlış konfiqurasiyası kimi şəbəkə avadanlığı problemi nəticəsində məhsuldarlıq anomaliyaları yarana bilər. Zərərli hərəkətlər təhlükəsizlik anomaliyaları ilə nəticələnən müntəzəm şəbəkə işini pozmaq məqsədi daşıyır. Təhlükəsizlik anomaliyaları altı növə bölünür (T. Zoppi, A. Ceccarelli, L. Salani, and A. Bondavalli, 2020): infeksiya, partlayıcı zond, fırıldaq, traversal və paralellik.

Birinci kateqoriya, infeksiya, zərərli fayllara quraşdırılaraq və ya onunla qarışaraq hədəf sistemini yoluxdurmaq məqsədi daşıyır. Bu kateqoriyaya viruslar və qurdlar daxildir. Bufer daşqınları kimi partlayan anomaliyalar hədəf sistemi qüsurlarla örtmək məqsədi daşıyır. Nmap kimi hücumların araşdırma kateqoriyası sistemin zəifliklərini aşkar etmək üçün ilk növbədə məlumat əldə etməyə çalışır.

Saxta və ya qeyri-adi abonentlərdən istifadə dördüncü hücum növünün ümumi xüsusiyyətidir. Ümumi fırıldaqçı hücumlara digərləri arasında IP saxtakarlığı və MAC saxtakarlığı daxildir. Beşinci növ hücumlar bütün potensial açarları uyğunlaşdırmaqla hədəf sistemi pozmaq məqsədi daşıyır. Brute force və lüğət hücumları bu kateqoriyada məşhur hücum növləridir.

Nəhayət, DDoS kimi paralel hücumlarda təcavüzkarlar sistemin və ya xidmətin imkanlarını aşan çoxlu sayda sorğular göndərməklə sistemi və ya xidməti yararsız hala gətirməyə cəhd edirlər. Müdaxilə və ya təhlükə informasiyaya daxil olmaq, məlumatı manipulyasiya etmək və ya sistemi etibarsız etmək üçün qəsdən və icazəsiz cəhddir (L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, 2018). Məsələn, xidmətdən imtina hücumları (DoS) hostun düzgün işləməsi üçün tələb olunan resurslarını tükəndirməyə çalışır. Qurdlar və viruslar şəbəkədəki digər hostları hədəf alır və onların nüfuzdan salınması isə məlum zəifliklərdən istifadə edərək hosta imtiyazlı giriş əldə edir.

3.2.2. Anomaliyaların aşkarlanmasında maşın təlimi alqoritmlərinin tətbiqi

Maşın təlimi (MT), şəbəkə trafikinin nümunələrinin analizi vasitəsilə şəbəkə anomaliyalarının aşkarlanması üçün istifadə edilə bilən güclü bir vasitədir, bu prosedur hər bir MT kateqoriyası üçün tamamilə fərqlidir. Hətta eyni MT modelində iki eyni verilənlər bazasından seçilmiş xüsusiyyətlər və çəkilərə görə məhsuldarlıq ML alqoritminin istifadə üsulundan fərqli ola bilər.

Daha çox xüsusiyyətlərin əldə edilməsi avtomatik olaraq daha yüksək məhsuldarlıq əldə etməyə imkan vermir, əksinə, modelin həddindən artıq uyğunlaşmasına səbəb ola bilər (S. Yeom, I. Giacomelli, M. Fredrikson, and S. Jha, 2018).

Verilənlərin hazırlanması, alqoritm seçimi, model təlimi, qiymətləndirmə, modelin təkmilləşdirilməsi və proqnozlaşdırılması anomaliyaların aşkarlanması üzrə nəzarət edilən maşın təlimi prosesinin addımlardır. Verilənlərin hazırlanması verilənlərin toplanmasından annotasiyaya qədər ən vacib və vaxt aparan mərhələdir Toplanmış ilkin verilənlər nəzarət edilən maşın təlimi alqoritmində analiz edilməsi üçün ilkin emal edilməlidir, yəni dublikat verilənlər aradan qaldırılmalı və xüsusiyyətlər çıxarılmalı və formatlaşdırılmalıdır ki, nəzarət edilən maşın təlimi alqoritmi onu başa düşə bilsin.

Bundan əlavə, hər bir nümunə toplusunda etiketlənmiş verilənlər qrupu yaratmaq üçün ona tətbiq olunan təsnifatlandırıcı var. Bir qrup etiketli verilənlər hazırlamaq üçün hər bir nümunəyə bir təsnifatlandırıcı əlavə edilir. Nəzarət edilən maşın təlimi alqoritminin seçilməsindən sonra, təlim dəstindən istifadə edərək proqnozlaşdırıcı öyrədilir və doğrulama dəsti ilə qiymətləndirilir. Nəzarət edilən maşın təlimi alqoritminin parametrləri qiymətləndirmənin nəticələrinə əsasən optimal nəticə əldə etmək üçün dəyişdirilə bilər. Nəhayət, təlim keçmiş model ilə real vaxtda nümunə proqnozu mümkündür (Thottan, M., and Ji, C., 2003).

Verilənlər dəstindəki bütün xususiyyətlərdən istifadə etmək əvəzinə daha çox təlim və proqnozlaşdırma üçün ən vacib xususiyyətlərdən istifadə etmək daha məqsədə uyğundur, çünki bu, modeli daha yaxşı başa düşməyə imkan verir və nəticə ilə güclü əlaqəsi olmayan xüsusiyyətləri süzür. Bəzən proqnozun dəqiqliyi artır, digər vaxtlar isə nəticə daha az əlverişli olsa belə, proqnozun pisləşməsi çox az olur. Bu, həm də təlim vaxtına və sistem resurslarına qənaət edir.

Anomaliyaların aşkarlanması üçün nəzarətsiz maşın təlimində etiketli verilənlər ilə heç bir təlim keçirilmədiyinə görə, verilənlərdə kənara çıxmaların aşkarlanması qeyri-adi davranışların nadir hallarda baş verməsi ilə bağlıdır. Nəzarətsiz maşın təlimində verilənlər etiketlənməyə ehtiyac olmadan toplanır və alqoritm tərəfindən başa düşülməsi üçün dəyişdirilir. Nəzarətsiz maşın təlimi, nəzarət edilən maşın təlimindən fərqli olaraq, verilənlərə əsaslanan və naməlum vəziyyətləri aşkarlaya bildiyi üçün hesablama baxımından çətin nümunələri təhlil edə bilər. Anomaliya xüsusiyyətinə və nəzarətsiz maşın təlimi alqoritminin prinsipinə əsasən, müəyyən xüsusi hücumun aşkar edilməsi ehtimalı daha yüksəkdir, yəni anomaliyaların aşkarlanması üçün uyğun alqoritmin seçilməsi də zəruridir (Varun Chandola, Arindam Banerjee, and Vipin Kumar, 2009). Üstəlik, xüsusiyyətlərin çıxarılması və normallaşdırılması adətən nəzarətsiz maşın təlimi tərəfindən klasterləşdirmə modellərinə göndərilməzdən əvvəl aparılır. Testdə həmişə IP ünvanı və baytların sayı kimi rəqəmsal məlumatlara üstünlük verilir, çünki onlar çoxluqda qiymətli məlumatdır.

Real tətbiq zamanı nəzarətsiz maşın təlimi olan klasterləşdirmə modelinin düzgünlüyünü qiymətləndirmək çətindir və nəticələr etibarsız ola bilər. Bununla belə,

etiketli verilənlər əsasında anomaliyaların aşkarlanmasında nəzarətsiz maşın təliminin məhsuldarlığının kifayət qədər qənaətbəxş olduğu sübut edilmişdir (J. Camacho, G. Maciá-Fernández, J. E. D. Verdejo,and P. García-Teodoro, 2014).

Nəzarətsiz maşın təlimi, xüsusən də naməlum hücumlarla mübarizə zamanı nəzarət edilən maşın təlimindən üstündür. Nəzarət edilən maşın təlimi modelləri təlim məlumatlarına etibar etdiyi üçün əlaqəli qeydlərin olmaması səbəbindən naməlum hücumlar keçə bilər və problemi aşkar etmək üçün nəzarətsiz maşın təlimi modelləri tələb olunur.

Yarı nəzarətli təlim təsnifat və reqressiya məsələlərinin həli üçün həm etiketlənmiş, həm də etiketlənməmiş verilənlərdən istifadə etməklə nəzarət edilən və nəzarətsiz təlimi birləşdirən maşın təlimidir. Yarı nəzarətli maşın təlimi əvvəlcə etiketlənmiş məlumatlardan istifadə edərək modeli öyrədir. Bu etiketlənmiş verilənlər bir neçə sinifdə ola bilər ki, bu da təlim dəstinin bütün hücum növlərinin nümunələrini ehtiva etdiyini göstərir və yaxud da normal nümunələr kimi bir sinifdə ola bilər. Bu zaman proqnozlaşdırıcı yalnız normal trafik tərəfindən öyrədilir və anomaliya trafiki təsnif etməlidir.

Yarı nəzarətli maşın təlimi real dünyada daha praktikdir, çünki o, minimal verilənlər dəsti əsasında olduqca dəqiq proqnoz verməyə imkan verir. Yarı nəzarətli maşın təlimi etiketlənmiş verilənlərin çatışmazlığını aradan qaldırır və modelin həyata keçirilməzdən əvvəl adekvat təlim keçməsini təmin edir, lakin etiketlənməmiş məlumatların yanlış təsnifatı modeli yanlış proqnozlaşdırmağa yönəldə bilər (J. Veeramreddy and K. Prasad, 2019).

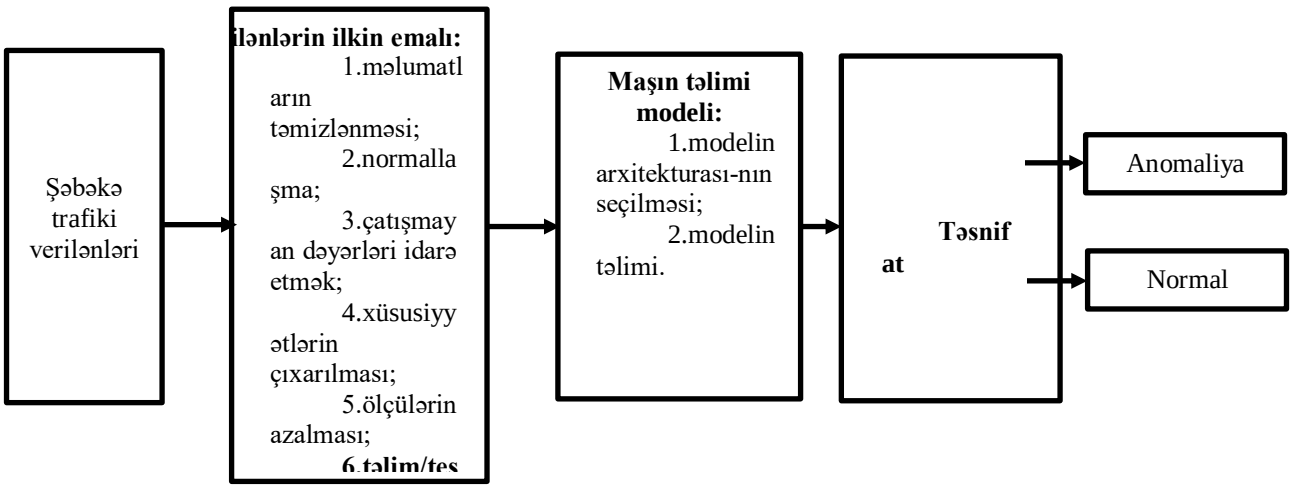
3.2.3. Anomaliyaların maşın təlimi əsasında aşkarlanmasının konseptual modeli

Anomaliyaların aşkarlanması üçün dərin təlimə əsaslanan konseptual model təklif edilir. Bu modeldə, şəbəkə trafiki verilənləri bloku şəbəkə trafiki haqqında məlumatları özündə cəmləşdirən kompüter şəbəkəsindən toplanmış ilkin xam verilənləri təmsil edir. Verilənlərin ilkin emalı bloku verilənlərin təmizlənməsi,

normallaşdırılması, çatışmayan dəyərlərin idarə edilməsi, xüsusiyyətlərin çıxarılması, ölçülərin azaldılması və təlim/test dəstinə bölünməsi kimi məsələləri əhatə edir. Bu mərəhələdə paket başlıqları, protokol növləri, paket ölçüləri, zaman və s. kimi xüsusiyyətlər çıxarılır, həmçinin, hesablama səmərəliliyini artırmaq və lazımsız məlumatları aradan qaldırmaq üçün xüsusiyyətlərin sayı azaldır. Bundan sonra, verilənlər toplusu təlim və test dəstlərinə bölünür. Maşın təlimi modelinin seçilməsi blokunda anomaliyaların aşkarlanması üçün uyğun olan maşın təlimi modelinin arxitekturası seçilir və təlim verilənləri üzərində öyrədilir.

Anomaliyaların aşkarlanması zamanı normal davranışdan əhəmiyyətli dərəcədə kənara çıxan halları müəyyən etmək üçün hədd (threshold) müəyyən edən anomaliya aşkarlama üsulları tətbiq edilir. Təlim edilmiş modelin məhsuldarlığı accuracy, precision, recall, F1-score və s. baxımından qiymətləndirmək üçün test dəsti əsasında qiymətləndirilir. Accuracy, precision, recall və F1-score kimi göstəricilər kompüter şəbəkələrində müdaxilələrin aşkarlanması modelinin effektivliyinin müəyyən edilməsi üçün hesablanır. Təsnifat mərhələsində anomaliyaların aşkarlanması üçün proqnozlaşdırılan "normal" və "anomaliya" sinif etiketləri üzrə təsnifat həyata keçirilir. Şəkil 3.7-də maşın təlimi əsasında anomaliyaların aşkarlanmasının konseptual modeli göstərilmişdir.

Kompüter şəbəkələrində anomaliyaların aşkarlanması üçün Random Forest modelinin istifadəsi təklif edilmişdir. Random Forest anomaliyaların aşkarlanması üçün çoxlu qərar ağaclarını birləşdirir. Hər bir qərar ağacı anomaliyaları müəyyən etmək üçün müəyyən xüsusiyyətlərə sadə təsnifatçı rolunu oynayır.



Şək. 3.7. Anomaliyaların maşın təlimi əsasında aşkarlanmasının konseptual modeli (Səməd Cabbarlı, Vüqar Stanbullu, 2024)

Bütün qərar ağaclarının eyni nümunələri öyrənməsinin qarşısını almaq üçün təsadüfilik tətbiq olunur. Qərar ağacları müxtəlif verilənlər alt dəstləri üzərində məşq edir və hər bölünmədə yalnız təsadüfi funksiyalar dəstini nəzərə alır. Yeni verilən nümunəsi gəldikdə bütün qərar ağacları onun təsnifatına (normal və ya anomaliya) səs verir və səs çoxluğu nəzərə alınır. Bu yanaşma Random Forest-i kənar göstəricilərə qarşı davamlı edir, onlara xüsusiyyətlər və anomaliyalar arasında mürəkkəb əlaqələri tutmağa imkan verir

3.2.3.1. İstifadə edilən verilənlər bazası və eksperimentin aparılması

Kompüter şəbəkələrində anomaliyaların aşkarlanması şəbəkə trafiki məlumatlarını ehtiva edən açıq verilənlər bazasının yüklənməsi və ilkin emalından başlayır. Verilənlərin bütövlüyünü təmin etmək üçün dataframe-də mövcud olan istənilən sonsuz dəyərlər NaN (nömrə deyil) ilə əvəz olunur, ardınca çatışmayan dəyərləri doldurmaq üçün interpolyasiya aparılır. Bu interpolyasiya itkin verilənlərin sonrakı analizinə təsirini azaltmağa kömək edir. Əlavə kəşfiyyat və modelləşdirmə üçün təmiz və tam verilənlər toplusunu təmin etmək üçün çatışmayan dəyərləri ehtiva edən hər hansı qalan sətirlər çıxarılır. Verilənlər toplusu 70%-i təlim toplusuna, qalan 30%-i isə test dəstinə ayrılır. Verilənlərin bu şəkildə bölünməsi model təlimini və qiymətləndirilməsini asanlaşdırır, sonrakı təhlillərin və proqnozların etibarlılığını artırır. Sonra TM modeli öyrədilir və şəbəkə trafikinin müxtəlif növlərinin təsnifatında modelin məhsuldarlığını qiymətləndirmək üçün müxtəlif ölçülər və vizuallaşdırmalar istifadə edilir. Modeli öyrətdikdən sonra həm train, həm də test məlumat dəstləri üçün proqnozlar yaradılır. Bu, məlumatların müxtəlif alt dəstləri üzrə anomaliyaların aşkar edilməsində modelin fəaliyyətinin qiymətləndirilməsinə imkan verir (Varun Chandola, Arindam Banerjee, and Vipin Kumar, 2009).

Eksperimentlərin aparılması üçün açıq olan CICIDS 2017 verilənlər bazasını istifadə edilmişdir. CICIDS 2017 verilənlər bazası müxtəlif növ kiberhücumlar və normal fəaliyyətlər üçün şəbəkə trafiki məlumatlarını ehtiva edən geniş istifadə olunan kibertəhlükəsizlik verilənlər toplusudur. Bu verilənlər bazası Nyu-Brunsvik Universitetinin Kanada Kibertəhlükəsizlik İnstitutu tərəfindən diqqətlə hazırlanmışdır, burada "normal" trafik və müasir ümumi kiberhücumlar var. Trafik məlumatları paketlərdən əldə edilir və CICFlowMeter istifadə edərək çıxarılır. Hər bir məlumat şəbəkə trafikinin xüsusiyyətlərinin 80-dən çox ölçülməsini ehtiva edir. O, müdaxilə aşkarlama sistemlərini qiymətləndirmək və müqayisə etmək məqsədi ilə yaradılmışdır. Verilənlər dəsti hər biri fərqli şəbəkə trafiki ssenarisini təmsil edir və bu ssenarilərə DDoS hücumları, port skanları, brute force hücumları və s. kimi müxtəlif növ hücumlar, həmçinin zərərli şəbəkə trafiki daxildir (Thottan, M., and Ji, C., 2003).

Logistic Regression və İsolation Forest modelləri Random Forest modeli ilə müqayisə etmək üçün CICIDS 2017 verilənlər bazasını istifadə etməklə öyrədilir və qiymətləndirilir. Bütün modellər Google Colab tərəfindən təmin edilən CPU sürətləndiricisindən istifadə etməklə Python 3.10.12-də Google Colab platformasında işlənilmiş və yoxlanılmışdır.

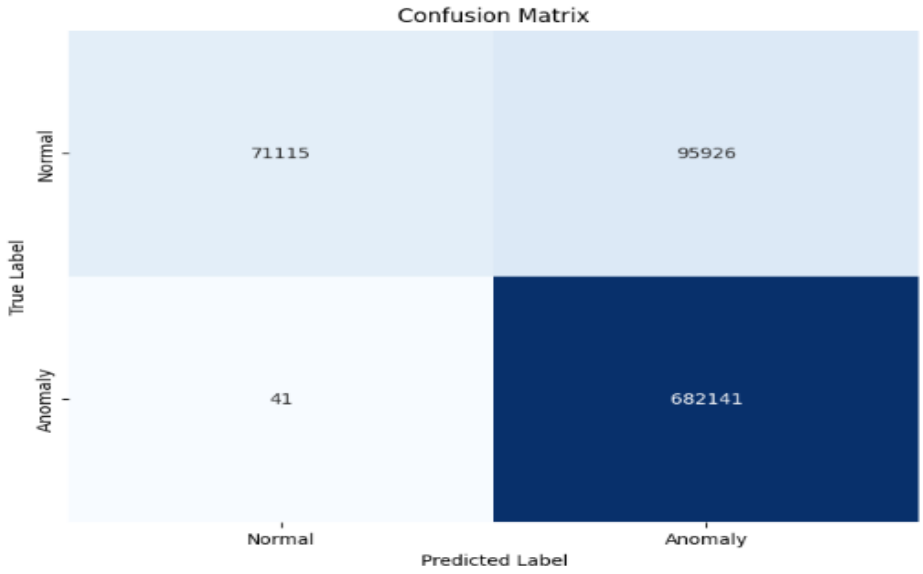
3.2.3.2. Eksperimental nəticələr və müzakirə

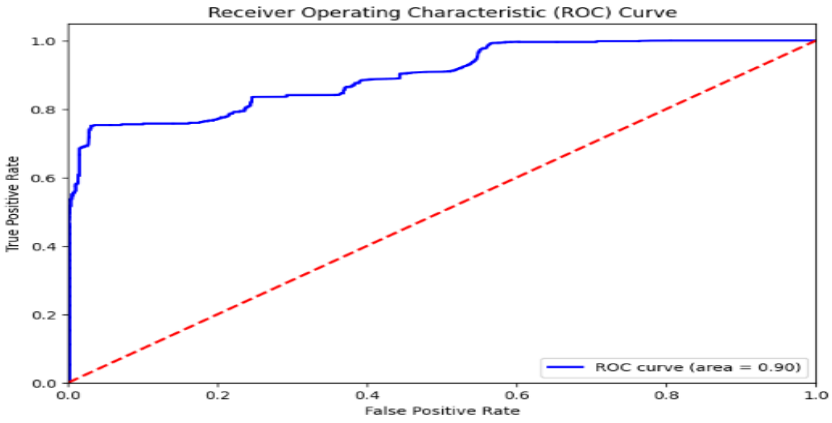
Random Forest, İsolation Forest və Logistic Regression modellərinin təlim prosesi qarışıqlıq matrisi və ROC əyri istifadə etməklə vizuallaşdırılmışdır (müvafiq olaraq 3.8, 3.9 və 3.10). Bu matrislər müxtəlif siniflər üzrə modelin məhsuldarlığının ətraflı qiymətləndirilməsinə imkan verən həqiqi pozitivlərin, həqiqi neqativlərin, yalançı pozitivlərin və yalan neqativlərin sayını göstərir. Təlimdən sonra Random Forest, İsolation Forest və Logistic Regression modelləri sınaqdan keçirildi və onların dəqiqliyi müvafiq olaraq 88.7%, 67.03%, və 87.37%-ə çatdı və buna görə də daha aşağı recall dərəcəsinə baxmayaraq, Random Forest daha yaxşı seçim ola bilər (Cədvəl 3.2).

Cədvəl 3.2. (Səməd Cabbarlı, Vüqar Stanbullu, 2024)

	Isolation Forest	**Logistic Regression**	**Random Forest**
Accuracy	67.03	87.37	**88.70**
Precision	33.24	84.23	**99.94**
Recall	67.10	44.04	42.57
F1 - score	44.46	57.84	**59.71**

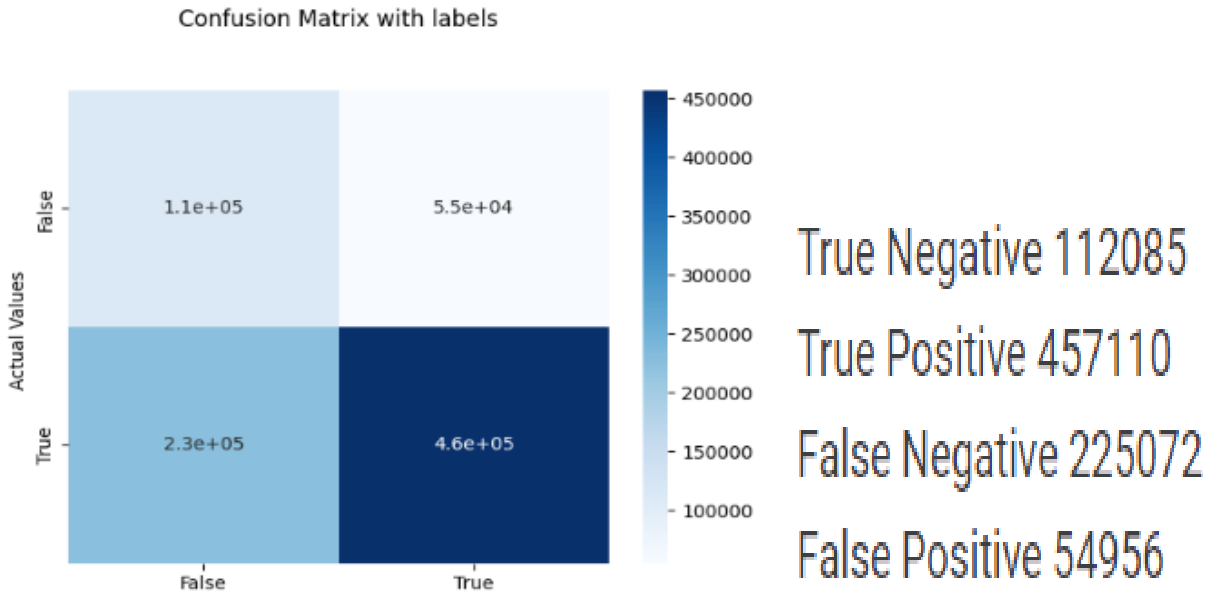
Bu o deməkdir ki, modellər test məlumatları üzərində dəqiq proqnozlar vermək üçün öyrədilib. Random Forest, İsolation Forest və Logistic Regression modellərinin məhsuldarlığı müxtəlif ölçülərdən istifadə etməklə qiymətləndirilmişdir. Isolation Forest orta accuracy, lakin daha aşağı precision və recall dərəcələri göstərdi, nəticədə daha aşağı F1-score əldə edildi. Logistic Regression Isolation Forest-dən daha yüksək accuracy nümayiş etdirdi, lakin daha az precision və recall nisbətlərinə sahib idi. O, precision və recall arasında daha yaxşı tarazlıq yaratdı və daha yüksək F1-score-a səbəb oldu. Random Forest accuracy və precision baxımından hər iki modeli üstələdi, lakin recall nisbəti daha aşağı idi. Buna baxmayaraq, o, üç model arasında ən yüksək F1 score əldə etdi ki, bu da ümumi məhsuldarlığının yüksək olduğunu göstərir.



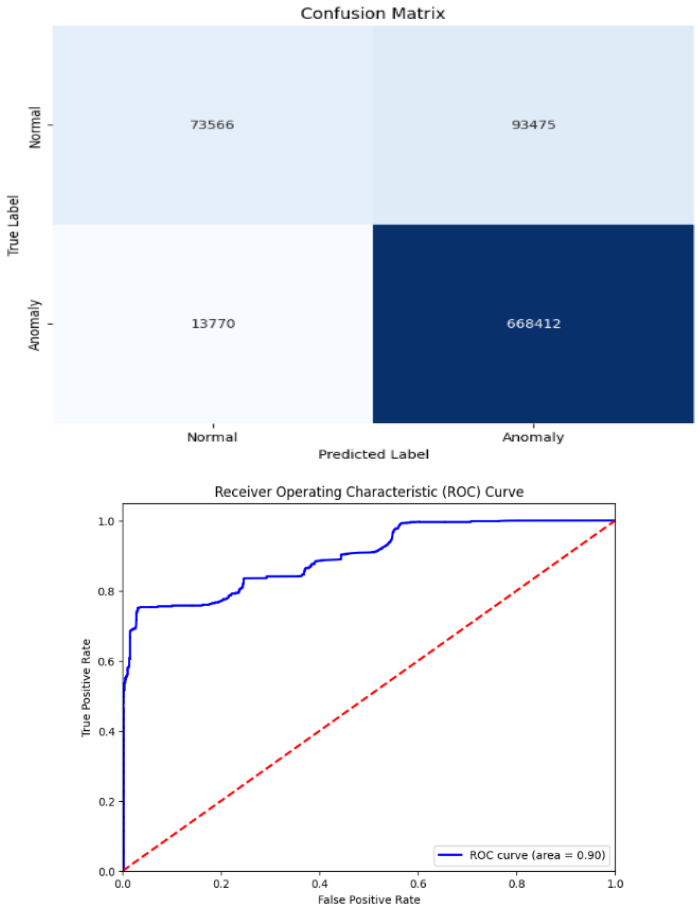


Şək. 3.8. Random Forest modeli üçün qarışıqlıq matrisi və ROC əyrisi (Səməd Cabbarlı, Vüqar Stanbullu, 2024)

Random Forest, İsolation Forest və Logistic Regression modellərinin qərar vermə prosesini vizuallaşdırmaq üçün təlim məlumatları üçün qərar funksiyası dəyərləri tərtib edilmişdir. Bu, modellərin normal və anomaliya halları necə fərqləndirdiyini anlamağa kömək edir.



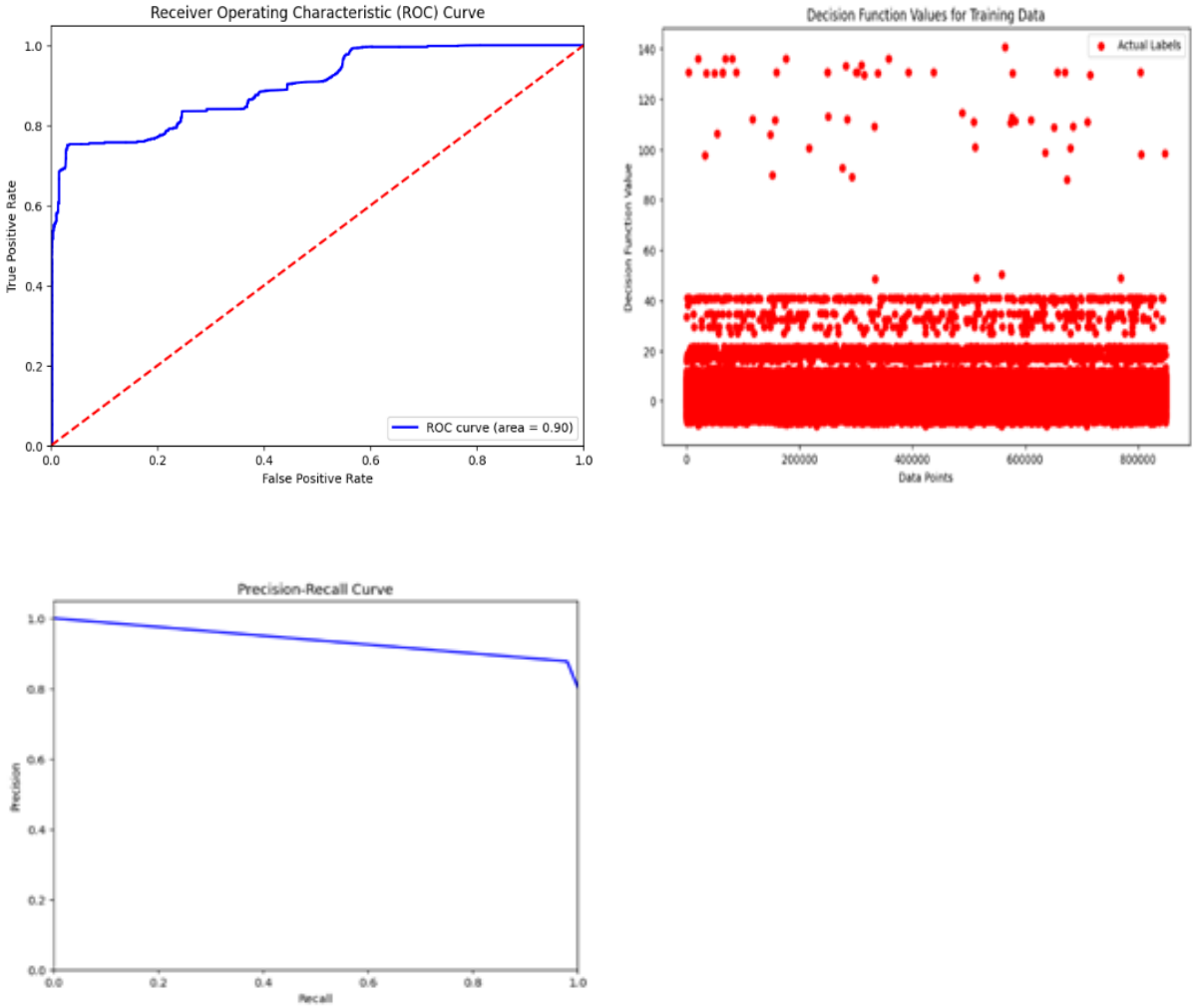
Şək. 3.9. Isolation Forest modelinin qarışıqlıq matrisi (Səməd Cabbarlı, Vüqar Stanbullu, 2024)



Şək. 3.10. Logistic regression üçün qarışıqlıq matrisi və ROC əyrisi (Səməd Cabbarlı, Vüqar Stanbullu, 2024)

ROC (Receiver Operating Characteristic) Curve: ROC əyriləri müxtəlif həddlər üzrə həqiqi müsbət nisbət (həssaslıq) və yanlış müsbət nisbət (1-spesifiklik) arasında uyğunluğu göstərmək üçün tərtib edilmişdir. ROC əyrisi (AUC) altında daha yüksək sahə daha yaxşı model məhsuldarlığını göstərir.

Precision-Recall (PR) Curve: Fərqli həddlər arasında precision və recall arasındakı əlaqəni nümayiş etdirmək üçün PR əyriləri yaradılmışdır. Bu vizuallaşdırma anomaliyaların aşkarlanması kimi balanssız verilənlər bazası ilə işləyərkən xüsusilə faydalıdır (Şəkil 3.11).

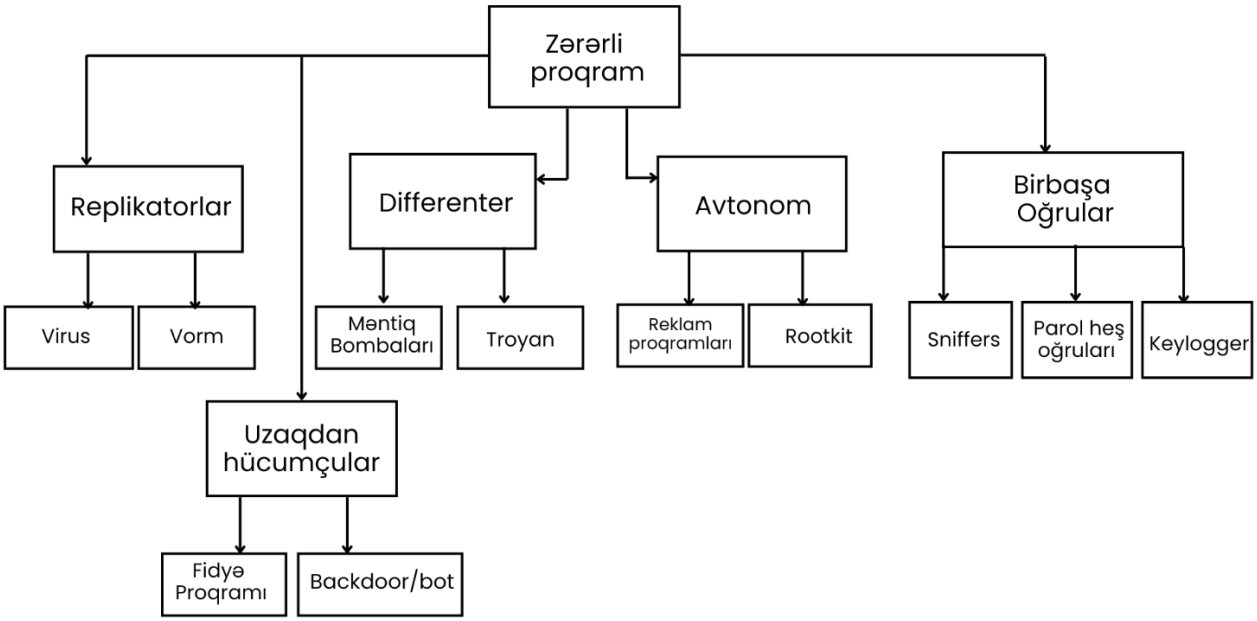


Şək. 3.11. ROC Curve, Decision Function Values, Precision-Recall Curve (Səməd Cabbarlı, Vüqar Stanbullu, 2024)

3.3. Kompüter şəbəkələrində zərərli proqramların dərin təlim əsasında aşkarlanması

Zərərli proqram kompüter və şəbəkələr üçün əhəmiyyətli təhlükədir, məlumatların pozulmasına, maliyyə itkisinə və sistemin çökməsinə səbəb ola bilər. Zərərli proqram təminatının mənzərəsini və onun kompüter şəbəkələrinə təsirini başa düşmək effektiv aşkarlama strategiyalarının işlənib hazırlanması üçün çox vacibdir. Zərərli proqramlar viruslar, şəbəkə soxulcanları, troyanlar və ransomware və digərləri daxil olmaqla geniş spektrli təhdidləri əhatə edir. Bu zərərli proqramlar müxtəlif vasitələrlə sistemlərə nüfuz edə, proqram təminatındakı boşluqlardan istifadə edə və ya istifadəçiləri aldada bilər.

Məqsədli olaraq pis niyyət üçün yaradılmış hər hansı proqram təminatı zərərli proqram kimi təsnif edilə bilər. Məqsəd və yayılma üsuluna görə təsnif edilə bilər (K.S., 2019). Şəkil 3.10-da zərərli proqramların təsnifatını göstərilmişdir. Zərərli proqramlar istifadəçilərin icazəsi və ya xəbəri olmadan özünü kopyalaya və kompüterləri yoluxdura, öz-özünü işə sala bilər.



Şək. 3.12. Zərərli proqramların təsnifatı (Vüqar Stanbullu, 2024)

Son illər ərzində zərərli proqramlar mürəkkəblik və gizlilik baxımından əhəmiyyətli dərəcədə təkamül edərək kibertəhlükəsizlik mütəxəssisləri üçün böyük problemlər yaratmışdır. Zərərli proqram təminatının aşkarlanmasının ənənəvi üsulları, məsələn, məlum nümunələri müəyyən etməyə əsaslanan siqnatura əsaslı yanaşmalar, yeni və polimorfik zərərli proqram təminatlarını aşkarlamaqda çətinlik çəkir. Normal davranışdan kənara çıxmaları müəyyən etmək məqsədi daşıyan anomaliya əsaslı aşkarlama üsulları zərərli və zərərsiz fəaliyyətləri dəqiq ayırmaqda müəyyən məhdudiyyətlərlə üzləşir. Bu problemləri həll etmək üçün tədqiqatçılar çoxsaylı aşkarlama üsullarını birləşdirən hibrid yanaşmalar təklif etdilər, lakin dəqiq və genişlənə bilən həllərin əldə edilməsi kibertəhlükəsizlik sahəsində aktual məsələ olaraq qalır.

Beləliklə, daim inkişaf edən təhdid mənzərəsi kompüter şəbəkələrində zərərli proqramların aşkarlanmasında problemlər yaradır. Əvvəlcədən müəyyən edilmiş

zərərli nümunələri müəyyən etməyə əsaslanan ənənəvi siqnatura əsaslı yanaşmalar sıfır gün hücumlarına qarşı təsirsiz olur. Bu, yeni təhdidlər təhlükəsizlik proqram təminatı siqnaturaların yenilənməsi ilə bağlı zəifliklərdən istifadə edir (John Smith, 2020). Digər tərəfdən, təcavüzkarlar şifrləmə, polimorfizm vasitəsilə zərərli kodları gizlədərək çaşqınlıq üsullarından fəal şəkildə istifadə edirlər (Sarah Thompson, 2018).

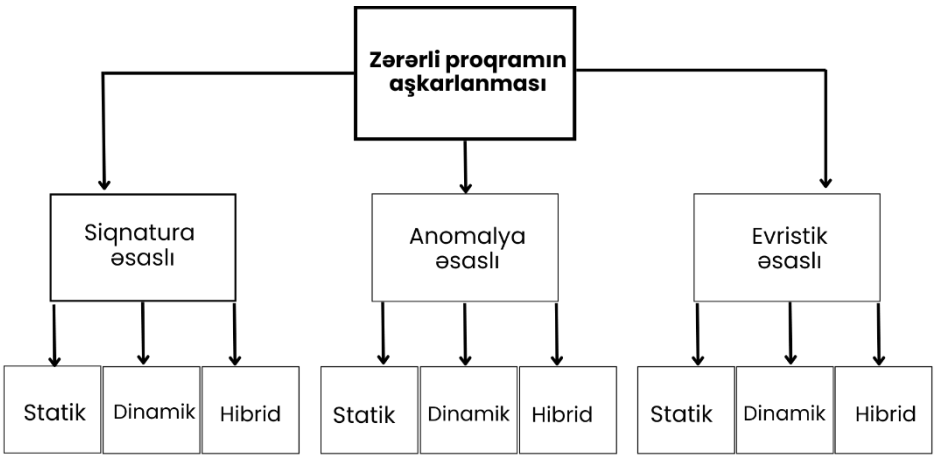
Aşkarlama səylərini daha da çətinləşdirən şifrələmənin geniş yayılmasıdır. Şifrləmə məlumatlarda şübhəli fəaliyyəti müəyyən etmək üçün şəbəkə trafikinin analizindən istifadə edərkən əhəmiyyətli dərəcədə maneə törədir.

Bu texniki maneələrdən əlavə, resurs məhdudiyyətləri də əhəmiyyətli problem yaradır. Bu da zərərli proqram təhlükələrinin getdikcə artan həcmi və mürəkkəbliyi ilə ayaqlaşmağı çətinləşdirir. Potensial zəifliklərin çoxluğu və yeni zərərli proqramların daim ortaya çıxması təhlükəsizliyə proaktiv yanaşma tələb edir.

Zərərli proqramların inkişaf edən təbiəti çox qatlı müdafiə strategiyasını tələb edir. Buraya siqnatura əsaslı aşkarlama, şübhəli hərəkətlər üçün proqram fəaliyyətinə nəzarət edən davranışa əsaslanan təhlil və idarə olunan mühitdə naməlum kodu təhlükəsiz şəkildə icra edən sandboxing üsulları daxildir. Əlavə olaraq, şəbəkə trafikində və sistem davranışında nümunələri müəyyən etmək üçün dərin təlim alqoritmlərindən istifadə yeni təhlükələrin aşkarlanmasında mühüm üstünlük təklif edə bilər. Məlumatlardan mürəkkəb nümunələri aşkarlamaq qabiliyyəti ilə dərin təlim, zərərli proqram təminatının tanınması üçün perspektivli bir üsul kimi görünür. Dərin təlim, şəbəkə trafikində mürəkkəb zərərli proqram davranışlarını aşkar etməkdə potensial üstünlüyə malikdir. Böyük həcmdə xam məlumatlardan mürəkkəb nümunələri və xüsusiyyətləri avtomatik aşkarlamaq üçün çox qatlı neyron şəbəkələrdən istifadə edilir ki, bu da zərərli proqramların aşkarlanması və digər kibertəhlükəsizlik məsələlərinin həlli üçün daha dəqiq və səmərəli həllər yaradılmasına imkan verər.

3.3.1. Zərərli proqramların aşkarlanmasının ənənəvi üsulları

Zərərli proqramların aşkarlanması üsulları siqnatura əsaslı, anomaliya əsaslı və evristik əsaslı olmaqla üç kateqoriyaya təsnif edilə bilər (Şəkil 3.13).



Şək. 3.13. Zərərli proqramların aşkarlanması üsullarının təsnifatı (Vüqar Stanbullu, 2024)

Siqnaturaya əsaslanan yanaşmalar proqram kodunda və ya davranışında siqnatura adlanan zərərli nümunələrin tanınması ilə əlaqədardır. Təhlükəsizlik proqram təminatçıları potensial təhlükələr üçün faylları və internet trafikini təhlil etmək üçün istifadə olunan bu siqnatura reyestrlərini yaradır (Faitouri A. Aboaoja, Anazida Zainal,Fuad A. Ghaleb,Bander Ali Saleh Al-rimy,Taiseer Abdalla Elfadil Eisa andAsma Abbas Hassan Elnour, 2022).

Siqnatura əsaslı aşkarlama üsulları müəyyən dərəcədə təhlükəsizlik təmin etsə də, əhəmiyyətli çatışmazlıqları vardır:

➢ Məhdud əhatə dairəsinə malikdirlər, yəni yalnız artıq məlum zərərli proqramları tanıya bilirlər. Zərərli proqramın mürəkkəb və məlum siqnaturası olmayan yeni variantlarını aşkar etmək çətin olur, çünki onların müəyyən edilmiş nümunəsi yoxdur;

➢ Yüksək dərəcədə yanlış müsbət səhvlərinin olması, yəni zərərsiz və zərərli proqram təminatları arasındakı oxşarlıqlar siqnaturaya əsaslanan sistemlərin nəticəni zərərli kimi yanlış şərh etməsinə səbəb ola bilər. Bu, əlavə pozulmalara və resursların israfına səbəb ola bilər;

➢ Daimi inkişaf etdirilməsi, yəni cari siqnatura verilənlər bazasını saxlamaq təhlükəsizlik təchizatçılarından daimi səy tələb edir. Bu, yavaş və resurs tutumlu ola

bilər ki, bu da zərərli proqramların ortaya çıxması ilə siqnaturanın yaradılması arasındakı müddət ərzində sistemlərin həssas olmasına səbəb olur.

Anomaliya əsaslı şəbəkə müdaxiləsinin aşkarlama yanaşmaları təhlükəsizlik problemlərinin həlli və şəbəkələri zərərli proqramlardan qorumaq üçün vacibdir (J. Camacho, G. Maciá-Fernández, J. E. D. Verdejo,and P. García-Teodoro, 2014). Anomaliyaya əsaslanan yanaşmalar, sistemin fəaliyyətinə təsnifat alqoritmlərini tətbiq etməklə hər hansı məlum və ya aşkar edilməmiş zərərli proqram təminatının müəyyən edilməsinə imkan verməklə, siqnatura əsaslı üsulların məhdudiyyətlərini yüngülləşdirir. Normal və ya anomaliya davranışı müəyyən etmək üçün nümunə əsaslı aşkarlamadan təsnifata əsaslanan yanaşmaya bu cür transformasiya zərərli proqram fəaliyyətlərinin aşkarlanmasında üstünlük verir (Varun Chandola, Arindam Banerjee, and Vipin Kumar, 2009).

Evristik əsaslı aşkarlama yanaşması: siqnatura və anomaliya əsaslı aşkarlama sistemləri üzərində Süni İntellektin tətbiqi zərərli proqramların aşkarlanmasının effektivliyini artırır. Proqnozlaşdırma qabiliyyətini artırmaq və ətraf mühitdəki dəyişikliklərə uyğunlaşmaq üçün təsnifatı yaxşılaşdırmaq üçün zərərli proqramların aşkarlanması sisteminə genetik alqoritm və neyron şəbəkəsi əlavə edilmişdir. Alqoritm sistem haqqında əvvəlcədən məlumatı olmadan çoxsaylı istiqamətlərdən optimal həllər əldə etmək üçün irsiyyət, seçim və birləşmə kimi xassələrdən istifadə edir (J. Camacho, G. Maciá-Fernández, J. E. D. Verdejo,and P. García-Teodoro, 2014). Statistik və riyazi metodologiyaların inteqrasiyası evristik metodu əvvəlki metodlardan üstün edir.

3.3.2. Zərərli proqramların aşkarlanmasında dərin təlimin tətbiqi

Dərin təlim, zərərli proqramların aşkarlanmasının ənənəvi üsullarının səmərəsizliyini aradan qaldırmaq üçün güclü bir üsuldur. Mürəkkəb nümunələri öyrənmək qabiliyyəti, zərərli proqram kodunun xüsusiyyətlərini daha dərin öyrənməyə imkan verir. Zərərli proqram təminatlarının aşkarlanmasında dərin təlimin əsas konsepsiyası həm zərərli proqram təminatı, həm də qeyri-intuitiv proqram təminatı ehtiva edən böyük verilənlər bazasından modellər yaratmaqdır. Bu verilənlər toplusuna proqramın kodundan (məsələn, bayt kodu ardıcıllığı), şəbəkə trafikinin

nümunələrindən və ya proqram tərəfindən edilən sistem xəbərdarlıqlarından əldə edilən xüsusiyyətlər daxil ola bilər. Bu xüsusiyyətlərin təhlili vasitəsilə dərin təlim modelləri zərərli və zərərsiz proqram təminatlarını fərqləndirə bilir (L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, 2018). Bu metodun bir sıra üstünlükləri var:

➢ Yüksək aşkarlama dəqiqliyinin olması, dərin təlim modelləri zərərli davranışın göstəricisi olan kiçik nümunələri tanımaqla əvvəllər heç vaxt görünməmiş zərərli proqram təminatlarının yeni variantlarını tanımaq potensialına malikdir;

➢ Aşağı dərəcədə yanlış müsbət səhvlərinin olması, zərərli və zərərsiz proqram təminatları arasındakı fərqlərin öyrənilməsi ilə dərin təlimi modelləri nəzəri olaraq yanlış pozitivlərin sayını azalda və aşkarlamanın dəqiqliyini artıra bilər;

➢ Uyğunlaşma, dərin təlim modellərinin dəyişiklikləri aşkar etmək imkanları yeni nümunələrdən öyrənməklə gücləndirilə bilər. Bu, onların zərərli proqram təminatlarının inkişaf edən mənzərəsinə uyğunlaşmasını asanlaşdırır.

Son illərdə tədqiqatçılar dərin təlimdən istifadə edərək zərərli proqramların aşkar edilməsini araşdırdılar. Vinayakumar və başqaları dərin təlim kimi mürəkkəb maşın təlim üsullarının zərərli proqramların aşkarlanmasında əl ilə xüsusiyyət mühəndisliyinə ehtiyacı necə azalda biləcəyini təsvir edir. Bununla belə, onlar vurğulayırlar ki, sonrakı tədqiqat tədqiqatları qeyri-obyektiv məlumatlar üzərində öyrədildikdə bu alqoritmlərin tətbiqində məhdudiyyətlər nümayiş etdirərək, real dünya şəraitində onların effektivliyini məhdudlaşdırır (L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, 2018).

Zərərli proqram hücumlarının sayı hər gün davamlı olaraq artır və bu da maliyyə faydaları hesabına artır. İlk müdafiə xətti Zərərli proqram aşkarlama sistemləridir (MDS). Zərərli proqramların aşkarlanması dağıdıcı hücumların qarşısını almaq üçün vacibdir. Zərərli proqram təminatının effektiv və dəqiq şəkildə aşkarlanması texnologiyaları. MDS ənənəvi maşın təlimi üsullarından istifadə edir. Bu, çox əmək tələb edən, xətaya meyilli xüsusiyyət seçimi və çıxarılmasını tələb edir. Şərti əsaslı dərin təlim tez-tez təkrarlanan API inyeksiyasına həssas olan Recurrent Neural

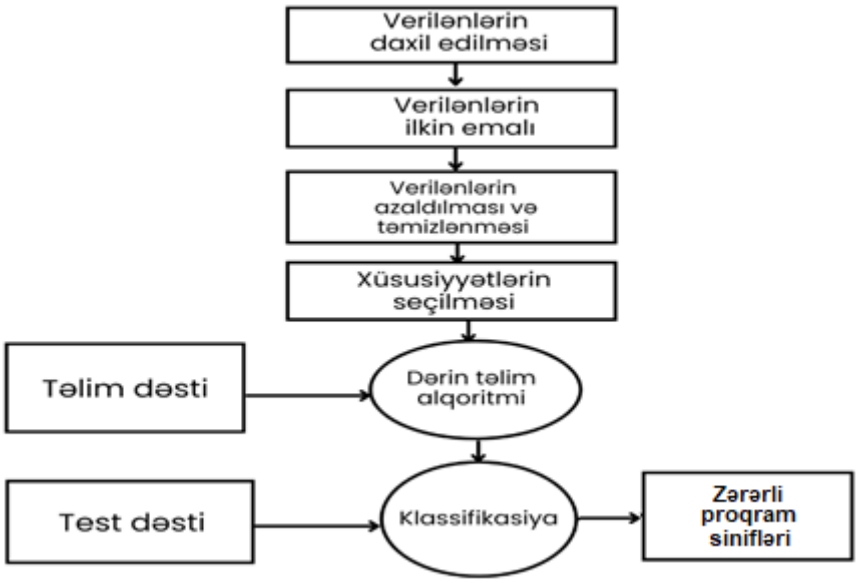
Network (RNN) istifadə edir. Bu araşdırma göstərir ki, Convolutional Neural Network (CNN) əsaslı zərərli proqramların aşkarlanması sistemi (MDS) lazımsız API inyeksiyalarına davamlı olmaqla zərərli proqram fayllarını tez və dəqiq təsnif etmək potensialına malikdir.

Araşdırmaya görə, yaxın gələcəkdə əşyalar bir-birinə bağlanmalı olacaq ki, bu da şəxsi məlumatların toplanmasına və çoxsaylı təhlükəsizlik riskləri və kibercinayətlərə səbəb ola bilər. Kibercinayətləri dayandırmaq üçün rabitədən əvvəl zərərli İnternet Protokolu (IP) ünvanlarını aşkarlaya bilən innovativ kibertəhlükəsizlik üsullarına ehtiyac var. Kiber-fiziki sistem üçün təhlükəsizlik risklərinin davranışını profilləşdirmək üçün istifadə edilən IP reputasiya sistemi ən yaxşı üsullardan biridir. Bu yanaşma həm də risk xallarını, ciddilik səviyyələrini, güvən reytinqlərini və təhlükənin nə qədər müddətə uyğun ola biləcəyini hesablayarkən böyük məlumatların məhkəmə ekspertizasının problemlərini həll edir. Sistemin effektivliyi iki mərhələdə qiymətləndirilir. Birincisi, müxtəlif maşın təlimi üsulları dəqiqlik, tamlıq və bu ikisinin balanslaşdırılmış ölçüsü (F-ölçüsü) baxımından ən yaxşı nəticələr verən birini tapmaq üçün müqayisə edilir. Sonra bütün reputasiya sistemi mövcud olanlarla müqayisədə qiymətləndirilir.

3.3.3. Zərərli proqramların dərin təlim əsasında aşkarlanmasının konseptual modeli

Zərərli proqramların aşkarlanması üçün dərin təlimə əsaslanan konseptual model təklif edilir. Bu model məlumatların ilkin emalı, xüsusiyyətlərin seçimi, təsnifat təlimi və zərərli proqramların aşkarlanması daxil olmaqla bir-neçə mərhələdən ibarətdir. Proses zərərli proqramlardan ibarət məlumat dəstlərinin toplanması, ilkin emalı və xüsusiyyətlərin seçilməsi ilə başlayır. Zərərli proqramları aşkar etmək üçün klassifikator öyrədilir. Normal və zərərli proqram nümunələri ayırd etmək üçün çıxış ehtimalına hədd (probability thresholding) tətbiq edilir. Təlim edilmiş modelin məhsuldarlığı accuracy, precision, recall, F1-score və s. baxımından qiymətləndirmək üçün test dəsti əsasında qiymətləndirilir. Accuracy, precision, recall və F1-score kimi göstəricilər kompüter şəbəkələrində müdaxilələrin aşkarlanması modelinin

effektivliyinin müəyyən edilməsi üçün hesablanır. Təsnifat blokunda anomaliyaların aşkarlanması üçün proqnozlaşdırılan zərərli proqram sinif etiketləri üzrə təsnifat həyata keçirilir. Şəkil 3.14-də dərin təlim əsasında zərərli proqramların aşkarlanmasının konseptual modeli göstərilmişdir.



Şək. 3.14. Zərərli proqramların dərin təlim əsasında aşkarlanmasının konseptual modeli (Vüqar Stanbullu, 2024)

3.3.3.1. İstifadə edilən verilənlər bazası və eksperimentin aparılması

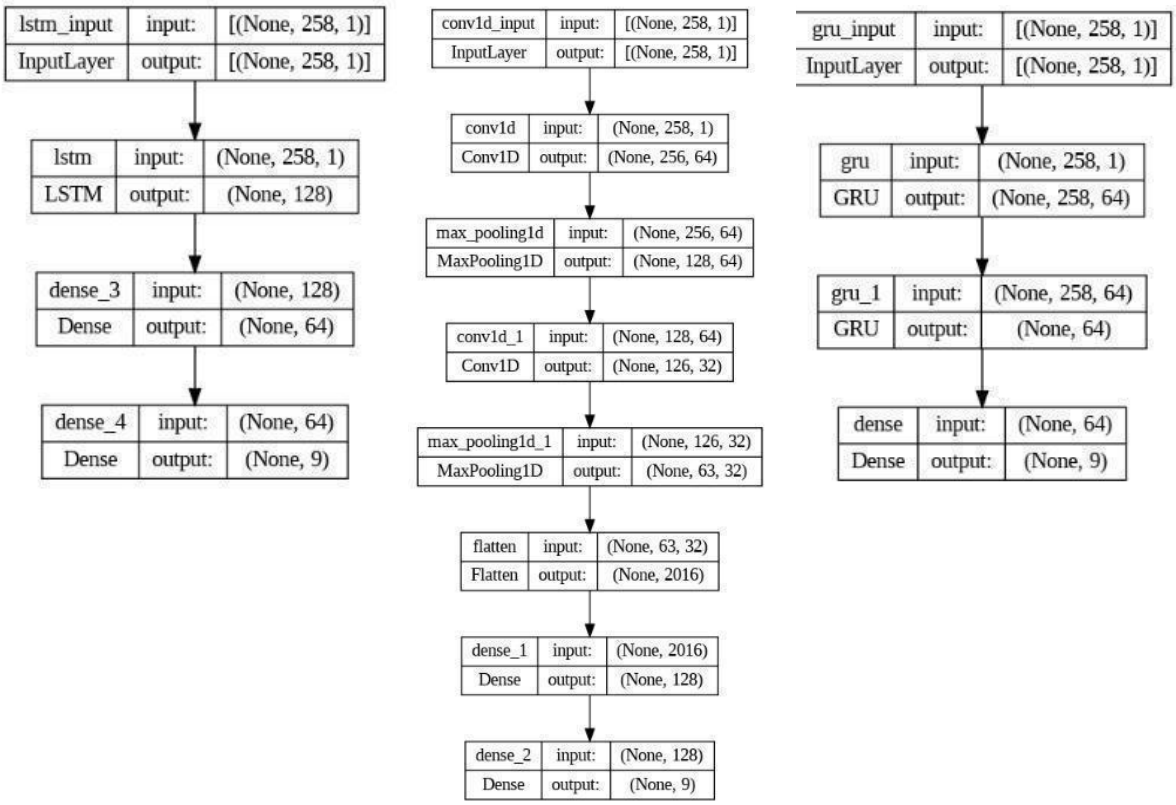
Microsoft Malware Classification Challenge (BIG 2015) verilənlər bazası zərərli proqramların tədqiqatı çərçivəsində geniş istifadə edilən verilənlər bazasıdır. 2015-ci ildə buraxılmış və 0,5 terabaytdan çox olan zərərli proqram nümunələrinin kolleksiyasıdır. 20000-dən çox zərərli proqram nümunəsi üçün asm və bayt kodu məlumatlarını ehtiva edən bu verilənlər bazası tədqiqatçılar üçün misilsiz bir fürsət təqdim edir. Verilənlər bazası doqquz fərqli ailəyə təsnif edilmiş məlum zərərli proqram fayllarından ibarətdir. Bu, kibertəhlükəsizlikdə mühüm məsələ olan zərərli proqramların avtomatlaşdırılmış aşkarlanması və təsnifatı üçün yeni üsulların işlənib hazırlanmasını və qiymətləndirilməsini asanlaşdırır. BIG 2015 verilənlər toplusbazasının böyük ölçüsü və müxtəlifliyi tədqiqatçılara zərərli proqram təhdidlərinin real təsviri üzərində öz modellərini öyrətməyə və qiymətləndirməyə imkan verir.

Kompüter şəbəkələrində zərərli proqramların aşkarlanması üçün Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Convolutional Neural Network (CNN) modelləri istifadə edilmişdir. Bu modellər BIG 2015 verilənlər bazasını istifadə etməklə öyrədilib və qiymətləndirilmişdir. Bütün modellər Google Colab tərəfindən təmin edilən CPU sürətləndiricisindən istifadə etməklə Python 3.10.12-də Google Colab platformasında işlənilmiş və yoxlanılmışdır.

3.3.3.2. Eksperimental nəticələr və müzakirə

Bu bölmədə zərərli proqramların aşkarlanması üçün LSTM, GRU və CNN modellərindən istifadənin eksperimental nəticələri təqdim olunur. Modellərin arxitekturaları şəkil 3.13-də göstərilmişdir. Hər bir model accuracy, precision, recall və F1-score kimi məhsuldarlıq göstəriciləri təhlil edilməklə müxtəlif zərərli proqram ailələrinin nümunələrini ehtiva edən verilənlər bazasında təlim keçmiş və qiymətləndirilmişdir. Bundan əlavə, qarışıqlıq matrisləri və təsnifat hesabatları modellərin imkanları və çatışmazlıqları haqqında əlavə məlumat verir. Verilənlər dəsti Ramnit, Lollipop, Kelihos_ver3, Vundo, Simda, Tracur, Kelihos_ver1, Obfuscator.ACY və Gatak daxil olmaqla müxtəlif növ zərərli proqram nümunələrindən ibarət idi.

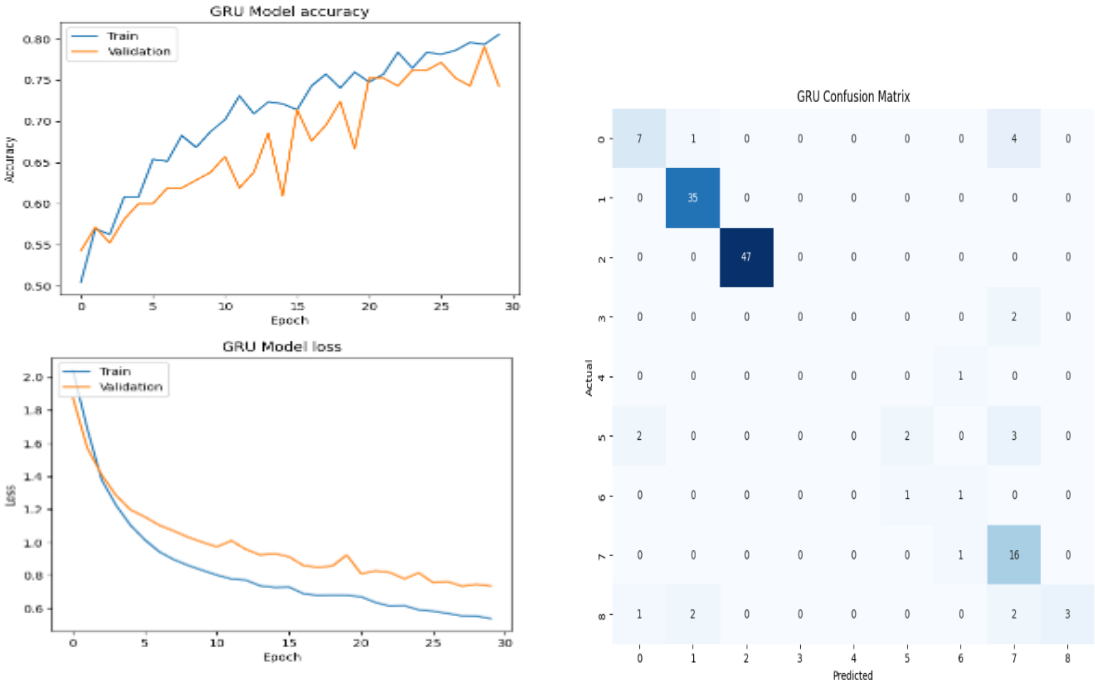
Hər bir model təlim və sınaq dəstlərinə bölünmüş eyni verilənlər toplusundan istifadə etməklə təlim keçmişdir. Biz hər model 30 dövr üçün 32 batch ölçüsü ilə təlim keçmişdir və Adam optimallaşdırıcısından istifadə edilmişdir.



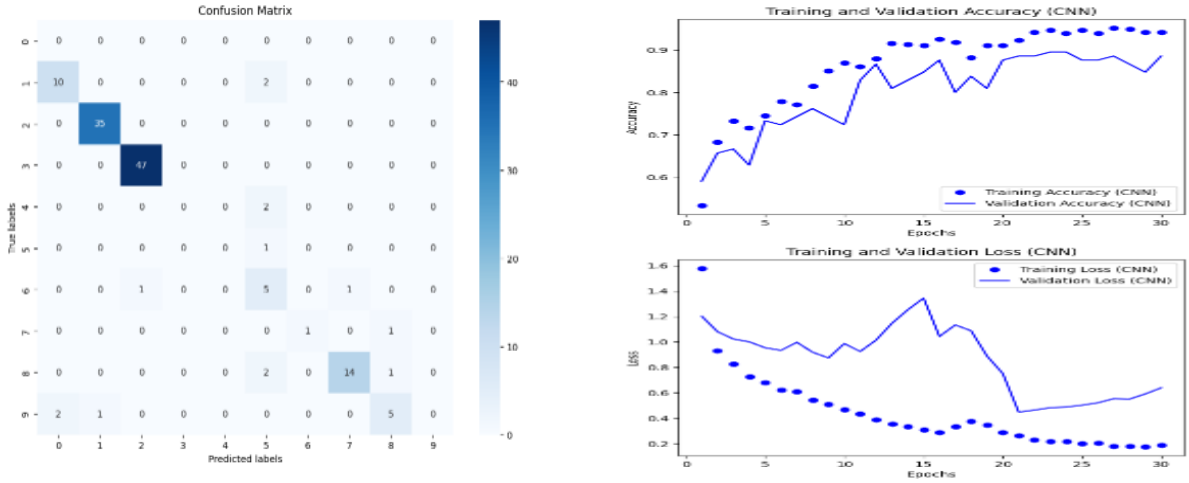
Şək. 3.15. LSTM, CNN və GRU modelinin arxitekturası (Vüqar Stanbullu, 2024)

GRU modeli sınaq dəstində 84,7% accuracy nümayiş etdirmişdi. Qarışıqlıq matrisinə əsasən demək olar ki, Lollipop və Kelihos_ver3 kimi zərərli proqram növlərinin düzgün aşkar edilməsində nəzərəçarpacaq məhsuldarlıq müşahidə etdirmişdi. Bununla belə, model Vundo və Tracur kimi müəyyən zərərli proqram siniflərini də aşkar edir. Bu model üçün precision, recall və F1 score təxminən 84,8%-dir ki, bu da siniflər arasında balanslaşdırılmış məhsuldarlığı göstərmişdir.

Qarışıqlıq matrislərindəki indekslər və onların uyğun gəldiyi zərərli proqram adları aşağıdakı kimi kodlaşdırılmışdır: 0 - Ramnit, 1 - Lollipop, 2 - Kelihos_ver3, 3 - Vundo, 4 - Simda, 5 - Tracur, 6 - Kelihos_ver1, 7 - Obfuscator.ACY və 8 - Gatak.



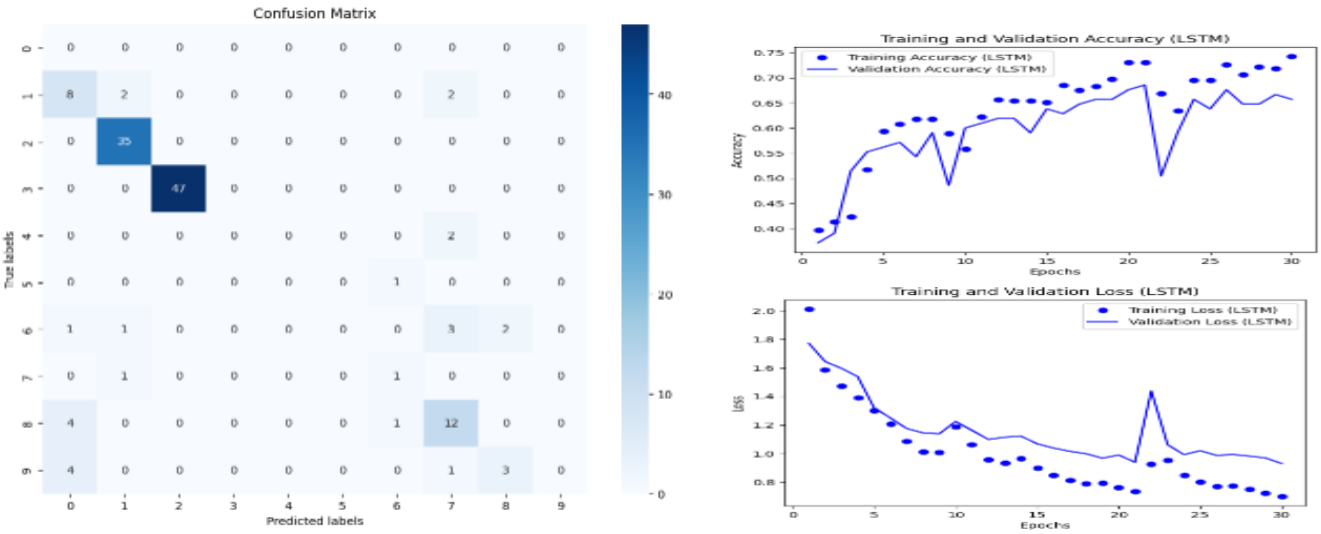
Şək. 3.16. GRU qarışıqlıq matrisi və accuracy /loss qrafiki (Vüqar Stanbullu, 2024)



Şək. 3.17. CNN qarışıqlıq matrisi və accuracy /loss qrafiki (Vüqar Stanbullu, 2024)

CNN modeli sınaq dəstində 89,3% yüksək accuracy nümayiş etdirmişdi. GRU modelinə nisbətən, Lollipop və Kelihos_ver3 zərərli proqram növlərinin aşkar edilməsində yüksək məhsuldarlıq nümayiş etdirmişdi. Bununla belə, o, həmçinin GRU modeli ilə müqayisədə 88,9% precision, recall və F1 score nümayiş etdirmişdi (Şəkil 3.17).

LSTM modeli sınaq dəstində 81,0% dəqiqliyə nail oldu. Həm GRU, həm də CNN modelləri ilə müqayisədə daha aşağı precision, recall və F1 nümayiş etdirmişdi. Model xüsusilə Ramnit və Tracur kimi müəyyən zərərli proqram siniflərini də aşkar edir. (Şəkil 3.18)



Şəkil 3.18. LSTM qarışıqlıq matrisi və accuracy /loss qrafiki (Vüqar Stanbullu, 2024)

Yekun olaraq, eksperimental nəticələrimiz CNN arxitekturasının sınaqdan keçirilmiş modellər arasında zərərli proqramların aşkar edilməsi məsələsi üçün ən effektiv olduğunu göstərir (Cədvəl 3.3)

Cədvəl 3.3. (Vüqar Stanbullu, 2024)

Model	**Accuracy**	**Precision**	**Recall**	**F1 Score**
GRU	84.73	84.77	84.73	82.84
CNN	**89.31**	**88.97**	**89.31**	**88.73**
LSTM	80.92	76.52	80.92	78.51

Cədvəl 3.4-də LSTM, GRU və CNN modellərindən istifadə etməklə zərərli proqramların təsnifat göstəricilərinin müqayisəsi göstərilir. Qiymətləndirmə meyarlarına accuracy,precision, F1 Score və recall daxildir.

Təcrübənin nəticələri göstərir ki, hər üç model Kelihos_ver3 zərərli proqramın aşkarlanmasında ən yüksək göstərici nümayiş etdirmişdir. Lakin hər üç model Vundo və Simda zərərli proqramları aşkarlaya bilməmişdir. Ümumilikdə, eksperimental nəticələr göstərir ki, CNN modeli GRU və LSTM modellərinə nisbətən zərərli proqramları aşkarlanmasında daha yaxşı işləyir.

Cədvəl 3.4. (Vüqar Stanbullu, 2024)

Traffic types	**Model**								
	GRU			**CNN**			**LSTM**		
	precision	**recall**	**f1-score**	**precision**	**recall**	**f1-score**	**precision**	**recall**	**f1-score**
Ramnit	0.57	0.67	0.62	0.79	0.92	0.85	0.41	0.58	0.48
Lollipop	0.95	**1.00**	0.97	0.94	0.91	0.93	0.89	0.94	0.92
Kelihos_ver3	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
Vundo	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Simda	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Tracur	0.40	0.29	0.33	0.57	0.57	0.57	0.00	0.00	0.00
Kelihos_ver1	**1.00**	0.50	0.67	**1.00**	0.50	0.67	0.33	0.50	0.40
Obfuscator.ACY	0.65	0.88	0.75	0.70	0.82	0.76	0.79	0.88	0.83
Gatak	0.75	0.38	0.60	0.50	0.50	0.50	0.38	0.38	0.38

NƏTİCƏ

Dissertasiya işi üzrə aparılmış tədqiqatlar zamanı qoyulmuş məsələlər həll edilmiş və aşağıdakı əsas elmi nəticələr əldə olunmuşdur:

1. Kompüter şəbəkələrinin kibertəhlükəsizliyi və monitorinq texnologiyaları analiz edilmişdir.
2. Süni intellektin əsas üsulları və onların kibertəhlükəsizlikdə tətbiqi məsələləri analiz edilmişdir.
3. Kompüter şəbəkələrində müdaxilələrin aşkarlanması üçün dərin təlim əsasında model işlənilmişdir.
4. Kompüter şəbəkələrində anomaliyaların aşkarlanması üçün maşın təlimi əsasında model işlənilmişdir.
5. Kompüter şəbəkələrində zərərli proqramların aşkarlanması üçün dərin təlim əsasında model işlənilmişdir.
6. Təklif olunmuş modellər təcrübi sınaqdan keçirilmiş, onların səmərəliliyi aparılmış eksperimentlər əsasında təsdiq olunmuşdur.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT

1. Abbasov, R. (2017). Kibertəhlükəsizlik: Mövzu, Müdaxilə və Yönləndirilmə. Bakı: Elm və Təhsil Nəşriyyatı.
2. Cavadov, V. (2019). Kibertəhlükəsizlik: Təcrübə və Təhlillər. Bakı: Nurlan Nəşriyyatı.
3. Imamverdiyev, Y., & Abdullayeva, F. (2018). Deep learning method for denial of service attack detection based on restricted Boltzmann machine. Big Data, 6(2), 159–169. https://doi.org/10.1089/big.2018.0023
4. Məmmədov, E. (2019). Süni Intellekt və Kibertəhlükəsizlik: İnnovasiyalar və Təhlükələr. Bakı: Tərəqqi Nəşriyyatı.
5. Nərimanova, S. (2021). Kibertəhlükəsizlik və Şəbəkə Təhlükəsizliyi İnkisi. Bakı: Qanun və Qadağanat Nəşriyyatı.
6. Quliyev, T. (2020). Süni Intellekt və Kibertəhlükəsizlik Müharibədə. Bakı: Dərviş Nəşriyyatı.
7. Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware detection issues, challenges, and future directions: A survey. Applied Sciences, 12(17), 8482.
8. Abeshu, A. Y., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2), 169–175.
9. Anderson, J. P. (1980). Computer security threat monitoring and surveillance (Tech. Rep.). Fort Washington, PA: James P. Anderson Co.
10. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In Proceedings of the 10th International Conference on Cyber Conflict (CyCon) (pp. 371–390).
11. Cai, J., Luo, J., Wang, S., & Yang, S. (2018). Feature selection in machine learning: A new perspective. Neurocomputing, 300, 70–79.

12. Camacho, J., Maciá-Fernández, G., D. Verdejo, J. E., & García-Teodoro, P. (2014). Tackling the Big Data 4 Vs for anomaly detection. In INFOCOM'2014 Workshop on Security and Privacy in Big Data (pp. 500–505).
13. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. https://doi.org/10.1145/1541880.1541882
14. Chung, J., Gulcehre, C., Cho, K., & Bengio, Y. (2014). Empirical evaluation of gated recurrent neural networks on sequence modeling. arXiv. https://arxiv.org/abs/1412.3555
15. Dua, S., & Du, X. (2016). Data Mining and Machine Learning in Cybersecurity. New York, NY, USA: Auerbach
16. Fraley, J. B., & Cannady, J. (2017, March). The promise of machine learning in cybersecurity. In Proceedings of SoutheastCon (pp. 1–6).
17. Géron, A. (2019). Hands-on machine learning with Scikit-Learn, Keras & TensorFlow: Concepts, tools, and techniques to build intelligent systems (2nd ed.). O'Reilly Media..
18. Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), 31–43.
19. He, K., & Kim, D. S. (2019, August). Malware detection with malware images using deep learning techniques. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 95-102). IEEE.
20. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9, 1735–1780.
21. ISO/IEC 2382. Information Technology Vocabulary.
22. Kebede, T. M., Djaneye-Boundjou, O., Narayanan, B. N., Ralescu, A., & Kapp, D. (2017, June). Classification of malware programs using autoencoders based deep learning architecture and its application to the Microsoft malware classification challenge (BIG 2015) dataset. In Proceedings of IEEE National Aerospace and Electronics Conference (NAECON) (pp. 70–75).

23. K.S. (2019). Impact of malware in modern society. Journal of Scientific Research and Development, 2, 593–600.
24. Kulkarni, A., & Brown, L. L., III. (2019). Phishing websites detection using machine learning. International Journal of Advanced Computer Science and Applications, 10(7), 8–13. https://doi.org/10.14569/IJACSA.2019.0100702
25. Maimo, L. F., Gomez, A. L. P., Clemente, F. J. G., Perez, M. G., & Perez, G. M. (2018). A self-adaptive deep learning-based system for anomaly detection in 5G networks. IEEE Access, 6, 7700–7712.
26. Martinez, J. (2018). Cybersecurity Monitoring: Leveraging AI and Machine Learning. San Diego: Routledge.
27. Meira, J., Andrade, R., Praça, I., Carneiro, J., Bolón-Canedo, V., Alonso-Betanzos, A., & Marreiros, G. (2020). Performance evaluation of techniques in cyber-attack anomaly detection. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4477–4489.
28. Michie, D., Spiegelhalter, D. J., & Taylor, C. (1994). Machine learning. Neural and Statistical Classification, 13.
29. Potluri, S., Ahmed, S., & Diedrich, C. (2018). Convolutional Neural Networks for Multi-class Intrusion Detection System. In Mining Intelligence and Knowledge Exploration (pp. 225–238). Springer, Cham.
30. Schuster, M., & Paliwal, K. K. (1997). Bidirectional recurrent neural networks. IEEE Transactions on Signal Processing, 45, 2673–2681.
31. Smith, J. (2020). Artificial Intelligence Applications in Cybersecurity Monitoring. London: Pearson Education.
32. Thompson, S. (2021). Advanced Techniques for Cybersecurity Monitoring using AI. San Francisco: Springer.
33. Thottan, M., & Ji, C. (2003). Anomaly detection in IP networks. IEEE Transactions on Signal Processing, 51(8), 2191–2204.
34. Veeramreddy, J., & Prasad, K. (2019, June). Anomaly-Based Intrusion Detection System.

35. Vincent, P., Larochelle, H., Lajoie, I., Bengio, Y., & Manzagol, P. A. (2010). Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. Journal of Machine Learning Research, 11, 3371–3408
36. Wilson, L. (2019). AI-Based Approaches to Enhancing Cybersecurity Monitoring. Seattle: Cambridge University Press.
37. Yeom, S., Giacomelli, I., Fredrikson, M., & Jha, S. (2018, July). Privacy risk in machine learning: Analyzing the connection to overfitting. In Proceedings of IEEE 31st Computer Security Foundations Symposium (CSF) (pp. 268–282).
38. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.
39. Zhang, H., Yu, X., Ren, P., Luo, C., & Min, G. (2019). Deep Adversarial Learning in Intrusion Detection: A Data Augmentation Enhanced Framework. arXiv. https://arxiv.org/abs/1901.07949
40. Zoppi, T., Ceccarelli, A., Salani, L., & Bondavalli, A. (2020). On the educated selection of unsupervised algorithms via attacks and anomaly classes. Journal of Information Security and Applications, 52, 102474.
41. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. https://doi.org/10.1145/1541880.1541882
42. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Robust intelligent malware detection using deep learning. IEEE Access, 7, 46717-46738.