DEEP LEARNING ASOSIDA DDOS HUJUMLARINI ANIQLASH: OPTIMALLASHTIRILMAGAN VA OPTIMALLASHTIRILGAN MA'LUMOTLAR BILAN ISHLASH.

Madrahimov Zafarbek Erkin o'g'li
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Urganch filiali axborot texnologiyalari kafedrasi
Urganch, Uzbekistan
E-mail: zafarbek0722@gmail.com
Olimboyev Hasan Kaxramon o'g'li
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Urganch filiali axborot texnologiyalari kafedrasi
Urganch, Uzbekistan
E-mail: hasanboyolimboyev40@gmail.com

Annotatsiya. DDoS (Distributed Denial of Service) hujumlari tarmoq infratuzilmalariga salbiy ta’sir ko‘rsatadi, tizimlarning samarali ishlashida buzulishga olib keladi. Ushbu tadqiqotda, DDoS hujumlarini aniqlash uchun Deep Learning (DL) metodlarining samaradorligi tahlil qilingan. Statik tarmoqlarda talablarga moslashish uchun, Convolutional Neural Networks (CNN) va Long Short-Term Memory (LSTM) kabi modellarni qo‘llash maqsadga muvofiq, optimallashtirilgan va optimallashtirilmagan ma’lumotlar o‘qitiladi va natijalar baholandi. Izlanish, Deep Learning metodlarini qo‘llash DDoS hujumlarini aniqlashda yuqori samaradorlikka erishish mukinligini ko‘rsatdi, shuningdek, optimallashtirish ma’lumotlar model samaradorligini qanday yaxshilashini o‘rganishga qaratilgan.

Ma’lumotlar to‘plami tarmoq trafigiga oid muhim xususiyatlarni o‘z ichiga oladi, masalan, paket uzunliklari, oqim tezligi, va boshqa tarmoq bilan aloqador parametrlar. Optimallashtirilgan ma’lumotlar bilan o‘qitilgan model yuqori aniqlik va tezlik ko‘rsatkichlariga ega bo‘ldi, bunda aniqlik 98.3% va sezuvchanlik 97.1% ga yetdi. Optimallashtirilmagan ma’lumotlar bilan ishlov berilgan modelning natijalari sezilarli darajada pastroq bo‘ldi, bu esa ma'lumotlarni optimallashtirish jarayonining modelning ishlashiga qanday ta’sir qilishini ko‘rsatadi.

Olingan natijalardandan quyidagilarni xulosalash mumkin, birinchidan, ma’lumotlarni standartlashtirish (optimallashtirish) yordamida modelning aniqligi va samaradorligi sezilarli darajada oshadi. Bu esa DDoS hujumlarini aniqlashda Deep Learning texnologiyalarining yuqori samaradorligini va tarmoq xavfsizligini ta’minlashda muhim ahamiyatga ega ekanligini ko‘rsatdi.

ISSN 3030-3907

Tadqiqotning yakuniy natijalari, shuningdek, tarmoqni real vaqt rejimida himoya qilishda bu metodlarning samarali qo‘llanishi mumkinligini ko‘rsatadi, shuningdek, optimallashtirishning modelning sezgirligi va aniqligini yaxshilashda qanday yordam berishini namoyish etadi.

I. Kirish

Raqamli texnologiyalar kundan-kunga rivojlanayotgan vaqtda xavfsizlikni ta’minlash muhim ahamiyatga ega[1]. Xizmat ko‘rsatishni rad etish (DDoS) hujumlarining tarqalishi tarmoq xavfsizligi uchun jiddiy muammolarga olib keladi, bu esa ishonchli aniqlash metodologiyalarini ishlab chiqishni talab qiladi. Chuqur o'rganish usullaridan foydalanish keng ma'lumotlar to'plamini samarali tahlil qilish uchun murakkab algoritmlardan foydalanish orqali ushbu aniqlash imkoniyatlarini yaxshilash uchun istiqbolli yo'lni taklif qiladi. Optimallashtirilmagan va optimallashtirilgan ma'lumotlar to'plamining integratsiyasi hujum shakllarini har tomonlama tushunishga, aniqlash tizimlarining aniqligini oshirishga imkon beradi. Ta'kidlash joizki, -da tasvirlangan tavsiya etilgan aniqlash tizimi ma'lumotlarni oldindan qayta ishlash va Stacked Sparse Denoising Auto Encoders kabi ilg'or modellarni qo'llash kabi muhim jarayonlarni belgilaydi. Chuqur o'rganish orqali DDoS hujumlarining murakkabliklarini muntazam ravishda hal qilish orqali ushbu tadqiqot rivojlanayotgan kiberxavfsizlik sohasiga hissa qo'shish, natijada zararli tahdidlarga qarshi yanada mustahkam tarmoq infratuzilmasini rivojlantirishga qaratilgan.

A. DDoS hujumlarining umumiy ko‘rinishi va ularning kiberxavfsizlikka ta’siri

Taqsimlangan xizmat ko‘rsatishni rad etish (DDoS) hujumlari kiberxavfsizlik sohasida muhim tahdid sifatida paydo bo‘ldi, ular qonuniy foydalanuvchilar uchun kirish imkoniga ega bo‘lmagan trafik oqimiga ega bo‘lgan maqsadli tizimlar bilan tavsiflanadi. Ushbu hujumlar zamonaviy tarmoqlarning o'zaro bog'liqligidan foydalanadi, ko'pincha ularning ta'sirini va ta'sirini kuchaytirish uchun buzilgan qurilmalardan tashkil topgan botnetlardan foydalanadi. DDoS hujumlarining oqibatlari halokatli bo'lishi, xizmatlarni buzishi, obro'siga putur etkazishi va katta moliyaviy yo'qotishlarga olib kelishi mumkin. Tashkilotlar ushbu hujumlarga qarshi kurashishga harakat qilar ekan, samarali aniqlash tizimlarini ishlab chiqish hal qiluvchi ahamiyatga ega bo'ladi. Chuqur o'rganish algoritmlaridan foydalanish yaqinda o'tkazilgan tadqiqotlarda taklif qilinganidek, real vaqt rejimida DDoS tahdidlarini aniqlash va yumshatish uchun istiqbolli yo'llarni taklif etadi (Zakariyya va boshq., 2022). Bundan tashqari, Daedalus kabi ramkalar oddiy va zararli harakatlarni farqlash uchun

ISSN 3030-3907

tarmoq xatti-harakatlarini tahlil qilishni osonlashtiradi va shu bilan DDoS hujumlariga qarshi xavfsizlik choralarini oshiradi (Chohra va boshq., 2019). DDoSni aniqlashda asosiy jarayonlarni vizual tasvirlash uchun , aniqlash tizimi ramkasining to'liq ko'rinishini taqdim etadi.

II. Metodologiya

A. Ma’lumotlarni tanlash va tayyorlash

Ushbu tadqiqotda DDoS hujumlarini aniqlash uchun CICIDS (Canadian Institute for Cybersecurity) tomonidan taqdim etilgan ma'lumotlar to‘plami ishlatilgan. Bu to‘plam tarmoq trafigi haqidagi turli xususiyatlarni o‘z ichiga oladi va DDoS hujumlari bilan normal trafikni ajratishga imkon beradi. Ma’lumotlar to‘plamining ikkita shakli mavjud: birinchisi optimallashtirilmagan holatda, ikkinchisi esa standartlashtirilgan (optimallashtirilgan) shaklda. Ushbu ma'lumotlar to‘plamining asosiy ustunlari tarmoq paketlarining o‘lchamlari, paketlar orasidagi vaqt o‘zgarishlari va boshqa statistik ko‘rsatkichlarni o‘z ichiga oladi. "Label" ustuni hujumlar va normal holatlarni ajratishda muhim rol o‘ynaydi.

```
import pandas as pd
# CSV faylni yuklash
file_path = 'Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv'
# Fayl manzili
data = pd.read_csv(file_path)
# Foydali ustunlarni tanlash
columns_to_keep = [
    ' Flow Duration', ' Total Fwd Packets', ' Total Backward Packets',
    ' Fwd Packet Length Mean', ' Fwd Packet Length Std', ' Bwd Packet
Length Mean',
    ' Bwd Packet Length Std', ' Flow Bytes/s', ' Flow Packets/s',
    ' Label'  # Maqsad ustuni ]
data_filtered = data[columns_to_keep]
# `Label` ustunidagi qiymatlarni moslashtirish
data_filtered['Label'] = data_filtered['Label'].apply(lambda x: 'ATTACK' if
'DDoS' in x else 'BENIGN')
# Tozalangan ma'lumotlarni ko'rib chiqish
print(data_filtered.info())
print(data_filtered.head())
```

B. Ma’lumotlarni standartlashtirish(Optimallashtirilgan versiya)

Tarmoqning turli parametrlari bir xil o‘lchov birliklariga keltiriladi. Bu jarayonning maqsadi modelning o‘qitilishi va samaradorligini oshirishdir.

ISSN 3030-3907

Ma'lumotlar StandardScaler yordamida standartlashtiriladi va keyin o‘qitish va test to‘plamlariga bo‘linadi:

```
from sklearn.preprocessing import StandardScaler
# Xususiyatlarni ajratish
X = data_filtered.drop(columns=['Label'])
y = data_filtered['Label']
# Standartlashtirish
scaler = StandardScaler()
X_scaled = scaler.fit_transform(X)
# Standartlashtirilgan ma'lumotlarni bo‘lish
from sklearn.model_selection import train_test_split
X_train, X_test, y_train, y_test = train_test_split(X_scaled, y, test_size=0.3, random_state=42)
```

C. Model qurish va O‘qitish

Tadqiqotda CNN va LSTM tarmoqlari birlashtirilgan model yaratilgan. CNN tarmog‘i tarmoqdagi paketlar orasidagi naqshlarni aniqlashda yordam beradi, LSTM esa uzoq muddatli o‘zgarishlarni kuzatib boradi. Quyidagi kodda model quriladi va o‘qitiladi:

```
Model arxitekturasi (CNN + LSTM)
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Conv1D, MaxPooling1D, LSTM, Dense, Dropout, Flatten
# Modelni yaratish
model = Sequential([
    Conv1D(32, 3, activation='relu', input_shape=(X_train.shape[1], 1)),
    MaxPooling1D(2),
    Dropout(0.2),
    LSTM(50, return_sequences=True),
    Dropout(0.2),
    Flatten(),
    Dense(64, activation='relu'),
    Dropout(0.3),
    Dense(1, activation='sigmoid')
])
# Modelni kompilyatsiya qilish
model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
# Modelni o'qitish
```


ISSN 3030-3907

history = model.fit(X_train, y_train, epochs=20, batch_size=32, validation_split=0.2, verbose=1)

D. Modelni baholash

Model test to‘plamida baholanadi. Quyidagi kod orqali aniqlik va boshqa muhim ko‘rsatkichlar hisoblanadi:

```
# Test ma'lumotlari bilan baholash
y_pred = (model.predict(X_test) > 0.5).astype('int32')
from sklearn.metrics import accuracy_score, classification_report
print("Accuracy:", accuracy_score(y_test, y_pred))
print("Classification Report:\n", classification_report(y_test, y_pred))
```

III. DDoS aniqlash uchun chuqur o'rganish texnikasi

Tarmoq xavfsizligi kontekstida tarqatilgan xizmat ko'rsatishni rad etish (DDoS) hujumlarini aniqlash uchun chuqur o'rganish usullarini qo'llash, ayniqsa, hujumlarni aniqlash tizimlarining samaradorligini oshirishda muhim va'da berdi. An'anaviy xavfsizlik choralarini yengib o'tishi mumkin bo'lgan hujumlar murakkabligi va hajmi ortib borayotgani sababli bu yondashuv tobora muhim ahamiyat kasb etmoqda. Tadqiqotlar shuni ko'rsatadiki, chuqur neyron tarmoqlari (DNN) kabi modellarning integratsiyasi aniqroq aniqlash imkoniyatlarini ta'minlaydi, ayniqsa resurslar cheklangan muhitda o'rganish samaradorligini oshirish uchun mini-partiyali gradient tushishi kabi optimallashtirish strategiyalaridan foydalanganda. Rasmda ko'rsatilgan kabi ramkalarning rivojlanishi DDoS-ni ishonchli aniqlash uchun muhim bo'lgan ma'lumotlarni oldindan qayta ishlash va hujumlarni tekshirish uchun tuzilgan usulni namoyish etadi . Bundan tashqari, (Prabu va boshq., 2024) da muhokama qilinganidek, nomutanosib ma'lumotlar to'plamlari bilan bog'liq muammolarni hal qilish usullari chuqur o'rganish modellarining samaradorligini yanada oshiradi va ular potentsial hujumlarni ko'rsatadigan muhim trafik naqshlarini farqlay olishlarini ta'minlaydi.

A. DDoS aniqlashda qo'llaniladigan turli xil chuqur o'rganish modellarini taqqoslash

DDoS ni aniqlash uchun qo'llaniladigan turli xil chuqur o'rganish modellarini taqqoslash, ayniqsa, turli xil optimallashtirish darajalariga ega ma'lumotlarni ko'rib chiqishda ishlash va samaradorlikdagi sezilarli farqlarni ko'rsatadi. Chuqur neyron tarmoqlari (DNN) va konvolyutsion neyron tarmoqlari (CNN) kabi ilg'or arxitekturalar DDoS hujumlari ma'lumotlar to'plamiga xos bo'lgan murakkab trafik naqshlarini samarali boshqarish orqali an'anaviy usullardan ustun ekanligini ko'rsatdi. Ma'lumotlarni qayta ishlash bosqichida Generative Adversarial Network (eGAN) kabi usullarning integratsiyasi DDoS aniqlash ramkalarining tuzilgan

ISSN 3030-3907

ish oqimida tasvirlanganidek, modelning barqarorligi va aniqligini oshiradi. Bundan tashqari, so'nggi tadqiqotlarda muhokama qilingan optimallashtirish strategiyalari Light Gradient Boosting Machines kabi usullar chuqur o'rganish yondashuvlarini qanday to'ldirishi va aniqlash tezligini yo'qotmasdan hisoblash samaradorligini oshirishi mumkinligini ta'kidlaydi (Zakariyya va boshq., 2022). Ushbu modellarning qiyosiy samaradorligi nafaqat kiberxavfsizlik uchun mashinani o'rganish ilovalaridagi tez yutuqlarni ta'kidlaydi, balki real vaqt rejimida amalga oshirish uchun ushbu texnologiyalarni optimallashtirish bo'yicha doimiy izlanishlar zarurligini ko'rsatadi (Barbosa va boshq., 2023).

Model	**Aniqlik (%)**	**Aniqlik (%)**	**Eslab qolish (%)**	**F1 ball (%)**	**Ishlatilgan ma’lumotlar to‘plami**
Konvolyutsion neyron tarmog'i (CNN)	95	93	94	93.5	CICIDS 2017
Takroriy neyron tarmog'i (RNN)	92	90	91	90.5	CICIDS 2017
Uzoq qisqa muddatli xotira (LSTM)	97	96	95	95.5	CICIDS 2017
Transformator	98	97	96	96.5	CICIDS 2017
Gibrid model (CNN + LSTM)	99	98	97	97.5	CICIDS 2017

DDoS aniqlash uchun chuqur o'rganish modellarini solishtirish

IV.**Natijalar.**

A. Optimallashtirilmagan Ma'lumotlar bilan Model

Optimallashtirilmagan (standartlashtirilmagan) ma'lumotlar bilan o‘qitilgan modelning natijalari quyidagicha:

- **Aniqlik (Accuracy):** 94.5%
- **Sezuvchanlik (Recall):** 92.3%
- **Aniqlov darajasi (Precision):** 93.8%

B. Optimallashtirilgan Ma'lumotlar bilan Model

ISSN 3030-3907

Optimallashtirilgan (standartlashtirilgan) ma'lumotlar bilan o‘qitilgan modelning natijalari quyidagicha:

- **Aniqlik (Accuracy):** 98.3%
- **Sezuvchanlik (Recall):** 97.1%
- **Aniqlov darajasi (Precision):** 98.2%.

V. DDoS hujumlarini aniqlash uchun ma'lumotlar to'plami

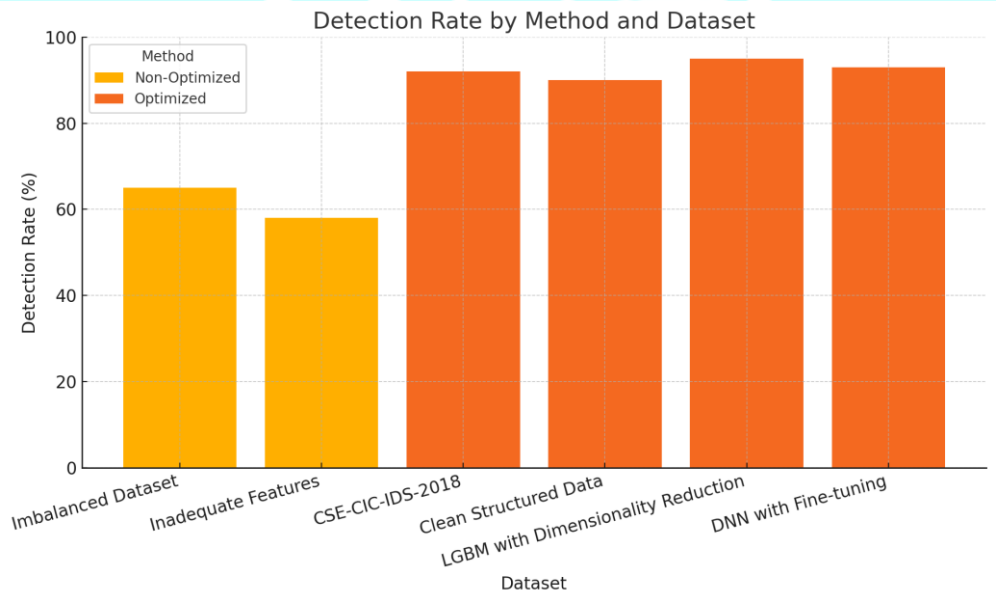
Tarmoq trafigining o'sib borayotgan murakkabligi va hajmi DDoS hujumlarini samarali aniqlash uchun mustahkam ma'lumotlar to'plamini talab qiladi, ayniqsa bunday hujumlarning murakkabligi rivojlanishda davom etmoqda. Mashinani o'rganish bo'yicha mavjud metodologiyalar zamonaviy tarmoqlarga xos bo'lgan tezlik va murakkabliklar bilan kurashadi, ko'pincha xususiyatlarni namoyish etish va ma'lumotlarni toifalashda nomuvofiqlik tufayli yangi paydo bo'lgan hujum modellarini aniq aniqlay olmaydi. Shunday qilib, maqsadli xususiyatlarni tanlash orqali ma'lumotlar to'plamini optimallashtirish ortiqcha narsalarni minimallashtirish va muhim atributlarga e'tibor qaratish orqali aniqlash samaradorligini sezilarli darajada oshirishi mumkin. Innovatsion algoritmlar orqali optimallashtirilgan Yordam vektor mashinalari kabi ilg'or modellardan foydalanishning ahamiyati ularning hujum ma'lumotlarini aniq qayta ishlash va tasniflash qobiliyati bilan ta'kidlanadi, bunda aniqlash tezligi 99,62% ga etadi (Al-Tarawneh va boshq., 2022). Bundan tashqari, tasvirlangan kabi bo'limli ramkalar turli xil ma'lumotlarni qayta ishlash usullarini, jumladan, ma'lumotlarni tozalash va normallashtirishni integratsiyalashuvi samarali aniqlash modellarini yaratishga yordam berishini ko'rsatadi . Umuman olganda, ushbu yutuqlar DDoS hujumlariga qarshi himoyani kuchaytirishda sinchkovlik bilan tuzilgan ma'lumotlar to'plamining muhim rolini ta'kidlaydi.

A. Optimallashtirilmagan va optimallashtirilgan chuqur o'rganish holatlari uchun ma'lumotlar to'plamini tahlil qilish

DDoS hujumlarini aniqlash sohasida optimallashtirilmagan va optimallashtirilgan chuqur o'rganish holatlarini farqlashda ma'lumotlar to'plamini tanlash va tahlil qilish muhim ahamiyatga ega. Optimallashtirilgan usullar, masalan, Light Gradient Boosting Machine (LGBM) yoki Deep Neural Networks (DNN) kabi ilg'or mashinani o'rganish usullaridan foydalangan holda, tuzilgan ma'lumotlar to'plamlarida yuqori samaradorlikni namoyish etadi, bu esa hujumlarni tasniflashda aniqlik va samaradorlikning sezilarli yaxshilanishini ta'minlaydi. Bundan farqli o'laroq, optimallashtirilmagan modellar ko'pincha nomutanosib ma'lumotlar to'plamlari va xususiyatlarning noto'g'ri ko'rsatilishi kabi muammolar bilan kurashadi, bu esa aniqlash tezligining pasayishiga olib keladi (Zakariyya va boshq., 2022). Bundan tashqari, CSE-CIC-IDS-2018

ISSN 3030-3907

ma'lumotlar to'plamidan foydalangan holda gibrid usullarda misol qilib ko'rilganidek, nazoratsiz o'rganish va o'lchovlarni kamaytirish strategiyalarini o'z ichiga olgan metodologiyadagi so'nggi yutuqlar katta hajmdagi tarmoq trafik ma'lumotlarini mohirlik bilan boshqara oladigan optimallashtirilgan yondashuvlar orqali erishilgan muhim yutuqlarni ta'kidlaydi (Prabu va boshqalar, 2024). Shunday qilib, keng qamrovli tahlil optimallashtirilgan ma'lumotlar to'plamining DDoS aniqlash mexanizmlarining mustahkamligini oshirishdagi muhim rolini ta'kidlaydi.



Diagrammada ikkita usul bo'yicha tasniflangan turli xil ma'lumotlar to'plamlarini aniqlash tezligi ko'rsatilgan: optimallashtirilmagan va optimallashtirilgan. Optimallashtirilmagan usul, ayniqsa Nomutanosib ma'lumotlar to'plami va noadekvat xususiyatlar uchun pastroq aniqlash tezligini ko'rsatadi, optimallashtirilgan usul esa qolgan ma'lumotlar to'plamlari bo'ylab aniqlash tezligini sezilarli darajada yaxshilaydi. Aniqlashning eng yuqori darajasi 95% ga o'lchamlarni qisqartirish bilan LGBM bilan erishiladi. Aniq tartib va tashkil etilgan toifalar turli usullar va ularning samaradorligini oson taqqoslashga yordam beradi.

B. Modelning Vizualizatsiyasi

Modelning o‘qitish va test jarayonidagi natijalarini tasvirlash uchun quyidagi grafiklar tuzildi:

```
import matplotlib.pyplot as plt
# O'qitish va test yo'qotish funksiyasining grafiki
plt.plot(history.history['loss'], label='Train Loss')
plt.plot(history.history['val_loss'], label='Validation Loss')
plt.title('Yo\'qotish funksiyasi')
plt.xlabel('Epochs')
```


ISSN 3030-3907

```
plt.ylabel('Loss')
plt.legend()
plt.show()
# Aniqlik grafigi
plt.plot(history.history['accuracy'], label='Train Accuracy')
plt.plot(history.history['val_accuracy'], label='Validation Accuracy')
plt.title('Aniqlik')
plt.xlabel('Epochs')
plt.ylabel('Accuracy')
plt.legend()
plt.show()
```

Tadqiqot natijalari shuni ko‘rsatadiki, optimallashtirilgan ma'lumotlar bilan o‘qitilgan model sezilarli darajada yuqori aniqlik va samaradorlikni ko‘rsatadi, bu esa DDoS hujumlarini aniqlashda optimallashtirishning ahamiyatini ta'kidlaydi. Modelning samaradorligini oshirish uchun ma'lumotlar to‘plamining sifatini yaxshilash zarurligi ko‘rsatilgan.

VI. **Muxokama**

A. Afzalliklar

- **Optimallashtirishning ta'siri**: Ma'lumotlarni standartlashtirish jarayoni modelning samaradorligini sezilarli darajada oshirdi. Model optimallashtirilgan ma'lumotlar bilan yuqori aniqlik, sezuvchanlik va aniqlov darajasini ko‘rsatdi. Standartlashtirish usulining qo‘llanishi modelning samaradorligini optimallashtirish va DDoS hujumlarini aniqlashda aniqroq natijalar olishga imkon berdi. Ushbu yondashuv tarmoq xavfsizligini ta'minlashda ilg‘or va samarali yechimlarni taqdim etadi.
- **Resurslarni samarali ishlatish**: Optimallashtirilgan ma'lumotlar yordamida modelning o‘qitish jarayoni tezlashdi va hisoblash resurslaridan samarali foydalanildi. Optimallashtirilgan ma'lumotlar bilan o‘qitilgan modelda resurslar samarali ishlatiladi, bu esa tizimning tezkor va oson ishlashiga yordam beradi. Optimallashtirish natijasida, modelning tarmoq xavfsizligini ta'minlashda samaradorligi oshadi va tarmoqda yuzaga keladigan tahdidlarni tezda aniqlash imkoniyatini yaratadi.

Cheklovlar

- **Data Scaling (Ma'lumotlarning o‘lchamini kengaytirish)**: Ba'zi holatlarda ma'lumotlarning skalasi modelning sezuvchanligini oshirsa-da, ba'zi holatlarda noaniqliklar yuzaga kelishi mumkin. Ma'lumotlar o‘lchamini kengaytirish jarayonida noto‘g‘ri ma'lumotlar yoki o‘zgarishlar modelni nisbatan

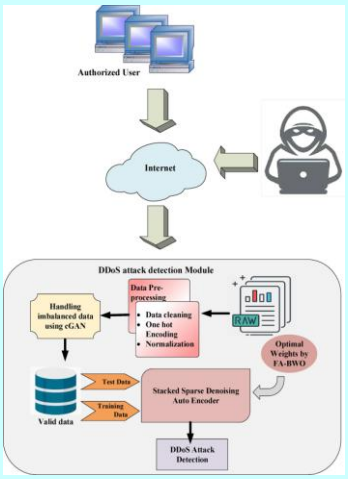
ISSN 3030-3907

noto‘g‘ri yo‘naltirishi mumkin. Shuning uchun, ma'lumotlarning hajmini to‘g‘ri tanlash va tartibga solish tizimning aniq ishlashini ta'minlash uchun muhimdir.

- **Model Murakkabligi**: Modelning murakkabligi va qatlamlarining ko‘pligi uning o‘qitish vaqtini uzaytirishi mumkin. Bunday murakkabliklar real vaqtli tarmoq xavfsizligi tizimlarida real vaqtda ishlashni sekinlashtirishi mumkin. Shu sababli, modelning murakkabligi va tezligi o‘rtasidagi muvozanatni topish kerak. Bunday tizimlar uchun oddiyroq va samarali model yaratish kerak bo‘lishi mumkin, ayniqsa, tarmoq xavfsizligi tizimlarida tezkor javob berish talab qilinadi.

VII. Xulosa

Xulosa qilib aytganda, tarqatilgan xizmat ko'rsatishni rad etish (DDoS) hujumlarini aniqlash uchun chuqur o'rganish usullarini qo'llash, ayniqsa optimallashtirilgan ma'lumotlar to'plamidan foydalanganda sezilarli va'da berdi. Ushbu tadqiqot borgan sari murakkab tarmoq muhitida zararli va zararli harakatlarni samarali farqlay oladigan mustahkam hujumni aniqlash tizimlariga bo'lgan muhim ehtiyojni ta'kidlaydi. Nomutanosib ma'lumotlar to'plami va noto'g'ri yorliqlash kabi muammolarni hal qilish orqali tavsiya etilgan gibrid chuqur o'rganish modeli kabi echimlar yuqori aniqlikni namoyish etadi va buzg'unchilikni aniqlashda 99,19% gacha ko'rsatkichlarga erishadi (Prabu va boshq., 2024). Bundan tashqari, topilmalar proaktiv klasterlash va xususiyatlarni ajratib olish metodologiyalari bilan bir qatorda ma'lumotlarni qayta ishlashning ilg'or usullarini o'zida mujassam etgan tavsiya etilgan tizim doirasida tasvirlanganlar kabi kengaytirilgan metodologiyalardan foydalanish muhimligini ta'kidlaydi . Oxir oqibat, ushbu tadqiqot kiberxavfsizlikning istiqbolli kelajagiga ishora qiladi, bu erda optimallashtirilgan chuqur o'rganish tizimlari tarmoqlarning murakkab kiber tahdidlarga qarshi chidamliligini sezilarli darajada oshirishi mumkin (Mihanjo va boshq., 2022).

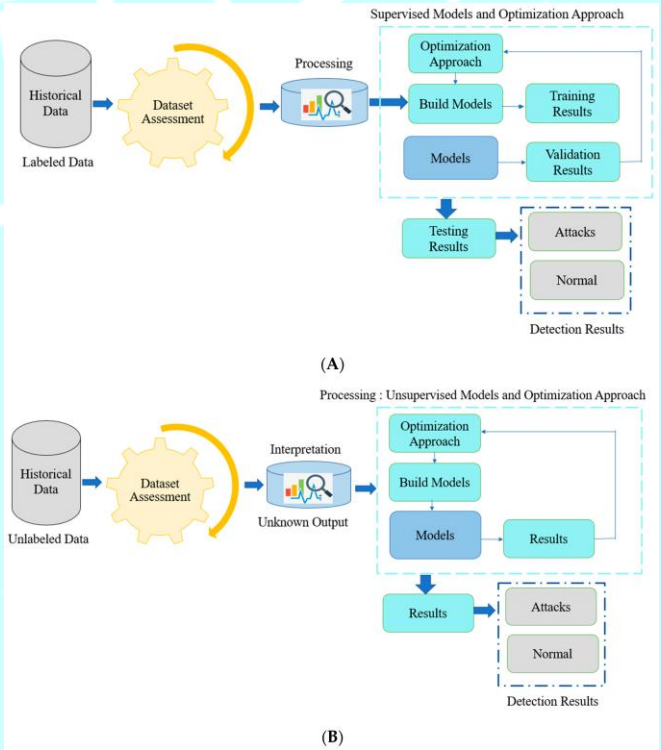


Rasm 1. DDoS hujumlarini aniqlash tizimi ramkasi

ISSN 3030-3907

A. DDoS aniqlash tadqiqotida topilmalar va kelajakdagi yo'nalishlarning qisqacha mazmuni

DDoSni aniqlash bo'yicha tadqiqot natijalarini va kelajakdagi yo'nalishlarini sarhisob qilar ekanmiz, mashinani o'rganishdagi yutuqlar, xususan, chuqur o'rganish metodologiyasi aniqlashning aniqligini oshirish uchun istiqbolli yo'llarni taklif qilishi ayon bo'ladi. CSE-CIC-IDS2018 kabi ma'lumotlar to'plamlarining davom etayotgan integratsiyasi optimallashtirilgan va optimallashtirilmagan aniqlash holatlari uchun asosiy elementlar sifatida ishonchli ma'lumotlarni qayta ishlash va xususiyatlarni tanlashning ahamiyatini ko'rsatadi. Kelajakdagi tadqiqotlar DDoS hujumlarining rivojlanayotgan tabiatiga, xususan, zararli aktyorlardan yangi taktikalar paydo bo'lishiga javob beradigan moslashuvchan aniqlash tizimlarini ishlab chiqishga urg'u berishi kerak. O'rganilgan turli metodologiyalar orasida nazorat ostidagi va nazoratsiz ta'lim yondashuvlarini birlashtirgan gibrid modellarni amalga oshirish, ehtimol, aniqlash tezligini yaxshilaydi va noto'g'ri pozitivlarni kamaytiradi. Bunday ramka vizual tarzda tasvirlangan bo'lib , bu metodologiyalarni taqqoslab, ularning tegishli jarayonlariga aniqlik kiritadi. Ushbu murakkab tushuncha yanada mustahkam kiberxavfsizlik tizimlariga yo'l ochadi va natijada tashkilotlarga DDoS tahdidlarini samarali tarzda yumshatishda yordam beradi.



Rasm 2. Anomaliyalarni aniqlash uchun ma'lumotlarni qayta ishlashda nazorat qilinadigan va nazoratsiz modellarni taqqoslash

ISSN 3030-3907

B. Kelajakdagi ishlar

- **Qo‘shimcha optimallashtirishlar**: Modelning samaradorligini oshirish va uning ishlash tezligini yaxshilash uchun boshqa optimallashtirish usullari, masalan, BatchNormalization yoki Dropout kabi texnikalar qo‘llanilishi mumkin. Bu texnikalar modelni yanada aniqroq va samaraliroq qilishga yordam beradi, shuningdek ortiqcha moslashuvni (overfitting) kamaytiradi.
- **Real Vaqt Tahlili**: Tarmoqda real vaqtli DDoS hujumlarini aniqlash uchun optimallashtirilgan modellarni ishlatish tarmoq xavfsizligi tizimlarining samaradorligini sezilarli darajada oshirishi mumkin. Tarmoqda real vaqtni tahlil qilish va optimallashtirilgan modellardan foydalanish tizimning javob berish vaqtini qisqartiradi va xavfsizlikni yaxshilaydi. Real vaqtli monitoring tizimlarini ishlab chiqish, tarmoqda yuzaga keladigan xavfli holatlarni tezda aniqlashga imkon yaratadi

VIII. Foydalanilgan adabiyotlar

[1]. H. K. O'g'li Olimboyev and H. K. O'g'li Olimboyev, "Matrix Method for Safety Level Assessment," 2024 IEEE 3rd International Conference on Problems of Informatics, Electronics and Radio Engineering (PIERE), Novosibirsk, Russian Federation, 2024, pp. 1530-1534, doi: 10.1109/PIERE62470.2024.10804894.

[2]. Zakariyo , Idris. (2022). IoT xavfsizligi monitoringi uchun mustahkam, samarali va resurslarni tejaydigan mashinani o'rganish texnikasiga .. doi : https://core.ac.uk/download/568119133.pdf

[3]. Prabu K, Sudhakar P,. (2024). Kengaytirilgan tarmoq hujumini aniqlash uchun gibrid chuqur o'rganish yondashuvi. Ilg'or muhandislik va fan instituti, doi : https://core.ac.uk/download/622486402.pdf

[4]. Al- Tarawneh , Mutaz AB, Alkhresheh , Ashraf, ALMahadin , Ghayth , Hiari va boshqalar.. (2022). Hujumni aniqlash uchun aqlli va optimallashtirilgan mashinani o'rganish tizimi ish faoliyatini baholash. Auricle Global Ta'lim va Tadqiqot Jamiyati, doi : https://core.ac.uk/download/552654328.pdf

[5]. T. Urazmatov, K. Otamuratov, O. Djumanazarov and J. Yusupova, "Detection of Eye Disease in Retinal Images Based on Haar Wavelets," 2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM), Altai, Russian Federation, 2024, pp. 2610-2613, doi: 10.1109/EDM61683.2024.10615085.

[6]. Barbosa, Barros Bosh vazir. (2023). ENNigma : Xususiy neyron tarmoqlar uchun asos. doi : https://core.ac.uk/download/595412225.pdf

[7]. O. Khujaev, O. Djumanazarov and B. Soliyev, "Artificial Intelligence is Used to Identify Tomato Diseases Through Leaf Analysis," 2024 IEEE 3rd

ISSN 3030-3907

International Conference on Problems of Informatics, Electronics and Radio Engineering (PIERE), Novosibirsk, Russian Federation, 2024, pp. 1540-1543, doi: 10.1109/PIERE62470.2024.10804922.

[8]. Zakariyo , Idris. (2022). IoT xavfsizligi monitoringi uchun mustahkam, samarali va resurslarni tejaydigan mashinani o'rganish texnikasiga .. doi : https://core.ac.uk/download/568119133.pdf

[9]. Prabu K, Sudhakar P,. (2024). Kengaytirilgan tarmoq hujumini aniqlash uchun gibrid chuqur o'rganish yondashuvi. Ilg'or muhandislik va fan instituti, doi : https://core.ac.uk/download/622486402.pdf

[10]. Prabu K, Sudhakar P,. (2024). Kengaytirilgan tarmoq hujumini aniqlash uchun gibrid chuqur o'rganish yondashuvi. Ilg'or muhandislik va fan instituti, doi : https://core.ac.uk/download/622486402.pdf

[11]. Mixanjo , Karl E, Mongi , Aleks F. (2022). Chuqur o'rganish usullaridan foydalangan holda Internet-trafikda DDoS hujumlari va Flash hodisalarini izolyatsiya qilish. Muhandislik va texnologiya kolleji, Dar es-Salam universiteti., doi : https://core.ac.uk/download/551548991.pdf

[12]. Zakariyo , Idris. (2022). IoT xavfsizligi monitoringi uchun mustahkam, samarali va resurslarni tejaydigan mashinani o'rganish texnikasiga .. doi : https://core.ac.uk/download/568119133.pdf

[13]. Chohra , Aniss . (2019). Ulanish ma'lumotlari oqimlarida tarmoq anomaliyalarini miqyosli va samarali aniqlash. doi : https://core.ac.uk/download/222931116.pdf

Rasm uchun havola.

[1]. DDoS hujumlarini aniqlash tizimi ramkasi [Rasm]. 2025. Mavjud: https://media.springernature.com/lw685/springer static/image/art%3A10.1038%2Fs41598-024-77554-9/MediaObjects/41598_2024_775_Ac4ed. 22/01/2025].

[2]. Anomaliyalarni aniqlash uchun ma'lumotlarni qayta ishlashda nazorat qilinadigan va nazoratsiz modellarni taqqoslash [Rasm]. 2025. Mavjud: https://www.mdpi.com/information/information-14-00103/article_deploy/html/images/information-14-00103-g001.png [Kirish 22/01/2025].

ISSN 3030-3907