

DEEP LEARNING ASOSIDA TARMOQ TRAFIGINI TAHLIL QILISH ORQALI KIBERHUJUMLARNI ANIQLASH

Usmanbayev Doniyorbek Shuxratovich¹, Raymqulova Gulzoda Ne'matjon qizi²

¹*Muhammad al-Xorazmiy nomidagi TATU katta o'qituvchisi*

²*Muhammad al-Xorazmiy nomidagi TATU talabasi*

ANNOTATSIYA. Mazkur tadqiqotda tarmoq trafigini deep learning (chuqur o'rganish) texnologiyalari asosida tahlil qilish orqali kiberhujumlarni aniqlash masalalari yoritilgan. Zamonaviy axborot tizimlarida tarmoq orqali uzatilayotgan ma'lumotlar hajmining keskin oshishi va murakkab kiberxavfsizlik tahdidlarining paydo bo'lishi an'anaviy himoya usullarining samaradorligini pasaytirmoqda. Deep learning asosidagi neyron tarmoqlar tarmoq trafigidagi yashirin naqshlarni aniqlash, anomal faoliyatni kuzatish hamda noma'lum kiberhujumlarni erta bosqichda aniqlash imkonini beradi. Tadqiqot natijalari kiberxavfsizlik tizimlarini takomillashtirish va intellektual tarmoq monitoringini joriy etishda muhim ahamiyatga ega.

Kalit so'zlar: deep learning, tarmoq trafigi, kiberhujumlar, kiberxavfsizlik, anomaliyalarni aniqlash.

ABSTRACT. This study focuses on detecting cyberattacks by analyzing network traffic using deep learning techniques. The rapid growth of network data and the increasing complexity of cybersecurity threats have reduced the effectiveness of traditional security approaches. Deep learning-based neural networks enable the identification of hidden patterns in network traffic, detection of anomalous behavior, and early recognition of unknown cyberattacks. The research findings contribute to improving cybersecurity systems and implementing intelligent network monitoring solutions.

Keywords: deep learning, network traffic, cyberattacks, cybersecurity, anomaly detection.

АННОТАЦИЯ. В данном исследовании рассматриваются вопросы обнаружения кибератак на основе анализа сетевого трафика с использованием технологий глубокого обучения (deep learning).

Стремительный рост объемов сетевых данных и усложнение угроз кибербезопасности снижают эффективность традиционных методов защиты. Нейронные сети, основанные на глубоком обучении, позволяют выявлять скрытые закономерности сетевого трафика, обнаруживать аномальную активность и своевременно определять неизвестные кибератаки.

Результаты исследования имеют важное значение для совершенствования систем кибербезопасности и интеллектуального мониторинга сетей.

Ключевые слова: глубокое обучение, сетевой трафик, кибератаки, кибербезопасность, обнаружение аномалий.

KIRISH

Raqamli texnologiyalarning jadal rivojlanishi va axborot tizimlarining globallashuvi natijasida kompyuter tarmoqlari orqali uzatilayotgan ma'lumotlar hajmi keskin oshib bormoqda. Shu bilan birga, kiberhujumlar soni va ularning murakkabligi ortib, axborot xavfsizligini ta'minlash zamonaviy jamiyatning eng dolzarb muammolaridan biriga aylanmoqda. Kiberjinoyatchilar tomonidan amalga oshirilayotgan zararli faoliyatlar tarmoq infratuzilmasiga, ma'lumotlar yaxlitligiga va foydalanuvchilar maxfiyligiga jiddiy tahdid solmoqda. An'anaviy kiberxavfsizlik usullari, jumladan signatura asosidagi aniqlash va qoidaviy filtratsiya tizimlari oldindan ma'lum bo'lgan hujumlarni aniqlashda samarali bo'lsa-da, yangi va noma'lum kiberhujumlarni aniqlashda yetarli darajada moslashuvchan emas. Ayniqsa, zero-day hujumlar va murakkab ko'p bosqichli tahdidlar mavjud sharoitda ushbu usullar o'z samarasini yo'qotmoqda.

Shu sababli, intellektual va avtomatik o'rganishga asoslangan yondashuvlarga ehtiyoj kuchaymoqda. Deep learning (chuqur o'rganish) texnologiyalari ko'p qatlamli neyron tarmoqlar yordamida katta hajmdagi tarmoq trafigi ma'lumotlarini chuqur tahlil qilish imkonini beradi. Ushbu yondashuvlar tarmoq trafigidagi yashirin naqshlarni aniqlash, normal va anomal faoliyatni farqlash hamda kiberhujumlarni erta bosqichda aniqlashda yuqori aniqlikni ta'minlaydi. Ayniqsa, konvolyutsion va rekurrent neyron tarmoqlar tarmoq trafigining vaqt va fazoviy xususiyatlarini o'rganishda samarali hisoblanadi. Mazkur ishda deep learning asosida tarmoq trafigini tahlil qilish orqali kiberhujumlarni aniqlashning nazariy asoslari, amaliy imkoniyatlari hamda kiberxavfsizlik tizimlaridagi ahamiyati yoritiladi. Tadqiqot natijalari zamonaviy axborot tizimlarida xavfsizlik darajasini oshirishga qaratilgan ilmiy-amaliy yechimlarni ishlab chiqishda muhim asos bo'lib xizmat qiladi.

MANBALAR MUNOZARASI

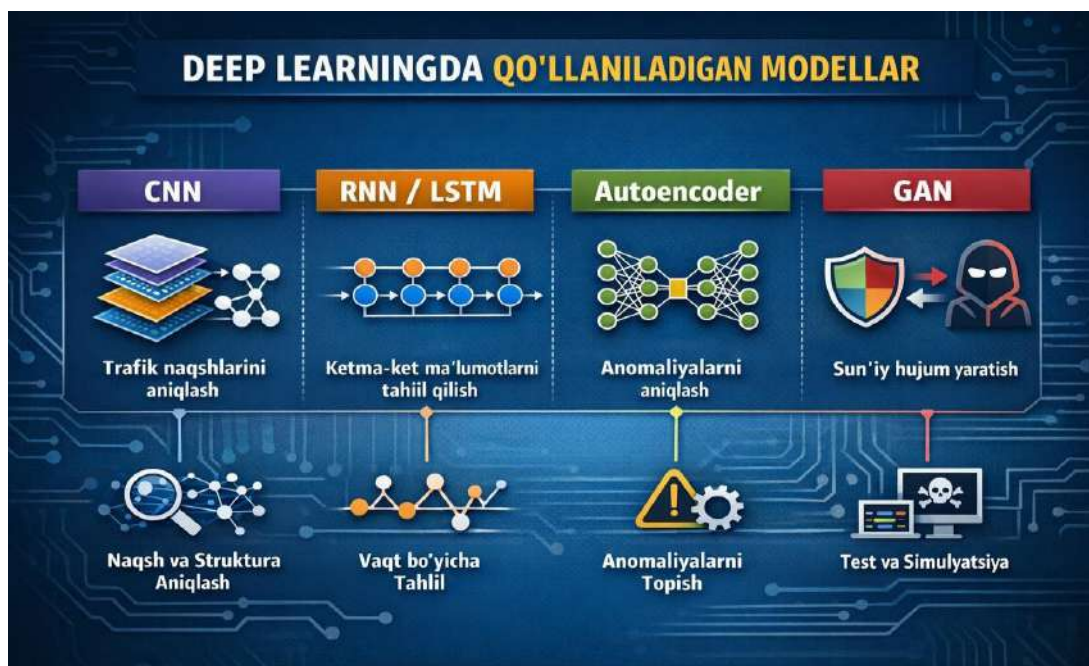
So'nggi yillarda tarmoq trafigini tahlil qilish va kiberhujumlarni aniqlash masalalari bo'yicha olib borilgan ilmiy tadqiqotlar soni sezilarli darajada oshdi. Ushbu tadqiqotlarning aksariyati sun'iy intellekt, xususan, mashinaviy o'rganish va deep learning texnologiyalariga asoslangan yondashuvlarni taklif etadi. Ilk ilmiy ishlarda kiberhujumlarni aniqlash asosan signatura va qoidaviy usullarga tayanib, oldindan ma'lum bo'lgan tahdidlarni aniqlashga qaratilgan edi. Biroq bu yondashuvlar yangi va noma'lum hujum turlarini aniqlashda yetarli darajada samarali emasligi bilan ajralib turadi. Keyingi tadqiqotlarda mashinaviy o'rganish usullaridan foydalanish kengayib, statistik modellarga asoslangan klassifikatsiya va klasterlash algoritmlari qo'llanila boshlandi. Ushbu

yondashuvlar an'anaviy usullarga nisbatan moslashuvchanroq bo'lsa-da, xususiyatlarni qo'lda tanlashga bo'lgan ehtiyoj va katta hajmdagi ma'lumotlar bilan ishlashdagi cheklovlar ularning asosiy kamchiliklari sifatida qayd etilgan. Zamonaviy ilmiy manbalarda deep learning asosidagi yondashuvlar tarmoq trafigin tahlil qilishda eng istiqbolli yo'nalish sifatida baholanmoqda.

Deep Learningda qo'yilgan modellar

Model turi	Vazifasi	Qayerda ishlatiladi
CNN	Naqsh va struktura aniqlash	Trafik paketlarini tasniflash
RNN	Ketma-ket ma'lumotlarni tahlil qilish	Vaqt bo'yicha trafik monitoringi
LSTM	Uzoq bog'lanishlarni o'rganish	Tarmoq sessiyalarini tahlil qilish
Autoencoder	Anomaliyani aniqlash	G'ayritabiiy trafikni topish
GAN	Sun'iy hujum yaratish	Tizimni test qilish

Tadqiqotchilar konvolyutsion neyron tarmoqlarni trafik paketlaridagi fazoviy xususiyatlarni aniqlashda, rekurrent neyron tarmoqlar va LSTM modellarni esa vaqtga bog'liq ketma-ketliklarni tahlil qilishda samarali deb hisoblashmoqda. Shuningdek, avtoenkoderlar asosidagi modellar noma'lum va zero-day kiberhujumlarni aniqlashda yuqori natijalar ko'rsatgani manbalarda ta'kidlangan.



2-rasm. Kiberxavfsizlikda Deep Learning modellari va ularning vazifalari.

Mahalliy (o‘zbek) ilmiy adabiyotlarda ham axborot xavfsizligi va tarmoq monitoringi masalalariga bag‘ishlangan ishlar mavjud bo‘lib, ularda kiberxavfsizlikni ta‘minlashda zamonaviy algoritmlarni joriy etish zarurligi qayd etilgan. Biroq aksariyat ishlarda deep learning modellarining amaliy qo‘llanilishi yetarli darajada chuqur yoritilmagan. Shu jihatdan, mazkur tadqiqot mavjud ilmiy bo‘shliqlarni to‘ldirishga va deep learning asosida kiberhujumlarni aniqlashning nazariy hamda amaliy jihatlarini kengroq ochib berishga qaratilgan. Tarmoq trafigi – bu kompyuter tarmoqlari orqali uzatiladigan ma’lumotlar paketlarining umumiy oqimi bo‘lib, uning monitoringi va tahlili tarmoq infratuzilmasi samaradorligi va xavfsizligini ta‘minlashda muhim ahamiyatga ega. Kiberhujumlar esa tarmoq trafigi orqali ma’lumotlar buzilishiga, tizimlarning ishlashini susayishiga yoki maxfiy ma’lumotlarning o‘g‘irlanishiga olib keladi. An’anaviy tahlil usullari, jumladan signatura va qoidaviy tizimlar, faqat oldindan ma’lum bo‘lgan tahdidlarni aniqlay oladi. Shu sababli, yangi va noma’lum kiberhujumlar aniqlanmay qolishi mumkin, bu esa zamonaviy tarmoqlarda xavfsizlik darajasini pasaytiradi.

NATIJALAR VA TAHLIL

Natija va Tahlil Elementlari	Tavsif
Umumiy samaradorlik	Deep learning modellarining samaradorligi an’anaviy usullardan sezilarli darajada yuqori.
CNN, RNN va LSTM ning roli	Murakkab naqshlarni aniqlash, normal va anomal trafikni ajratish imkonini beradi.
Avtoenkoderlarning afzalligi	Zero-day va noma’lum kiberhujumlarni aniqlash sezilarli darajada oshadi.
Real vaqt monitoring imkoniyati	Tarmoq xavfsizligini sezilarli darajada mustahkamlashga yordam beradi.
Yashirin naqshlarni aniqlash	Tarmoq trafigidagi yashirin naqshlarni aniqlash va anomal faoliyatni kuzatish imkonini beradi.
Noma’lum va zero-day hujumlarni erta aniqlash	Noma’lum kiberhujumlarni erta bosqichda aniqlashda yuqori aniqlik ta’minlaydi.
Qo‘shimcha imkoniyatlar	Trafik xatti-harakatlarini bashorat qilish, resurslarni samarali ishlatish va aqlli monitoring tizimlarini yaratishda samarali vosita.
Umumiy ahamiyat	Ilmiy va amaliy jihatdan tarmoq xavfsizligini oshirish, kiberxavfsizlik tizimlarini takomillashtirish va intellektual monitoringni joriy etishga xizmat qiladi.

XULOSA

Xulosa qilib aytganda, deep learning asosida tarmoq trafiginı tahlil qilish orqali kiberhujumlarni aniqlash zamonaviy axborot tizimlarida xavfsizlik darajasini oshirishning samarali yondashuvi hisoblanadi. Deep learning modellarining asosiy afzalligi shundaki, ular tarmoq trafigidagi yashirin naqshlarni aniqlash va anomal holatlarni sezishda yuqori aniqlik beradi. Zero-day va noma'lum kiberhujumlarni aniqlashda deep learning texnologiyalari an'anaviy usullardan ustunlikka ega.

Mezoni	An'anaviy usul	Deep Learning
Yangi hujum	Aniqlay olmaydi	Aniqlaydi
Tezlik	O'rtacha	Yuqori
Aniqlik	O'rtacha	Yuqori
Moslashuvchanlik	Past	Juda yuqori
O'zini o'rganish	Yo'q	Ha

Natijalar amaliy jihatdan tarmoq monitoringi, xavfsizlik tizimlarini takomillashtirish va aqlli tizimlarni joriy etishda muhim ahamiyatga ega. Shu bilan birga, tarmoq trafigi va kiberxavfsizlikni chuqur tahlil qilish uchun deep learning yondashuvlari zamonaviy IT infratuzilmalarda keng qo'llanilishi tavsiya etiladi. Ushbu ish natijalari ilmiy-amaliy asos sifatida kelajakdagi tadqiqotlar va amaliy loyihalar uchun muhim baza yaratadi.

FOYDALANILGAN ADABIYOTLAR:

- [1]. Qodirov A.A. Sun'iy intellekt asoslari. – Toshkent: O'zbekiston, 2019.
- [2]. Karimov Sh.X., To'rayev B.B. Axborot xavfsizligi va kiberxavfsizlik asoslari. – Toshkent: Fan va texnologiya, 2020.
- [3]. Islomov D.Sh. Kompyuter tarmoqlari va ularning xavfsizligi. – Toshkent: Innovatsion rivojlanish nashriyoti, 2021.
- [4]. Abdullayev A.R. Mashinali o'rganish va deep learning texnologiyalari. – Toshkent: Oliy ta'lim nashriyoti, 2022.
- [5]. Jo'rayev M.M., Rahmonov S.A. Axborot tizimlarida ma'lumotlarni tahlil qilish. – Toshkent: Fan, 2018.
- [6]. Xudoyberdiyev N.N. Kompyuter tarmoqlarida trafikni tahlil qilish usullari. – Toshkent: Texnika oliy ta'lim muassasalari uchun o'quv qo'llanma, 2020.
<https://api.ziyounet.uz/uploads/books/49959/60b0d1bd9d057.pdf>
- [7]. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Kiberxavfsizlikni rivojlantirish konsepsiyasi. – Toshkent, 2022.