Taraqqiyot spektri
ILMIY JURNALI
Vol 2 № 6 2026

SUN'IY INTELLEKT ASOSIDAGI KIBERXAVFSIZLIK TIZIMLARIDA ANOMALIYALARNI ANIQLASHNING YANGI USULLARI

Tursunov Bekzod Axrorovich

Namangan shahar 2-son texnikum maxsus fan o'qituvchisi

Mirzaxmedov Baxodir Mirzamurotovich

Namangan shahar 2-son texnikum maxsus fan o'qituvchisi

Buvamirzayeva Gulchiroy Olimjon qizi

Annotatsiya: Mazkur maqolada sun’iy intellekt (SI) texnologiyalari yordamida kiberxavfsizlik tizimlarida anomaliyalarni aniqlashning zamonaviy va samarali usullari tahlil qilingan. Hozirgi kunda kiberhujumlarning murakkablashib borishi an’anaviy qoidaga asoslangan himoya tizimlarining ojizligini ko‘rsatmoqda. Maqolada chuqur o‘rganish (Deep Learning), neyron tarmoqlar va avtokoderlar yordamida tarmoq trafigidagi g‘ayritabiiy holatlarni real vaqt rejimida aniqlash mexanizmlari o‘rganilgan. Tadqiqot doirasida ma’lumotlar to‘plamini qayta ishlash, xususiyatlarni ajratib olish va modelning aniqligini oshirishga qaratilgan yangi yondashuvlar taklif etilgan. Olingan natijalar SI asosidagi tizimlar kiberxavfsizlikda noto‘g‘ri ijobiy (false-positive) natijalarni kamaytirish va tahdidlarni erta bosqichda bartaraf etishda yuqori samaradorlikka ega ekanligini tasdiqlaydi.

Kalit so‘zlar: Sun’iy intellekt, kiberxavfsizlik, anomaliyalarni aniqlash, chuqur o‘rganish (Deep Learning), neyron tarmoqlar, tarmoq xavfsizligi, kiberhujumlar, ma’lumotlar tahlili, mashinali o‘qitish.

Kirish

Zamonaviy raqamli iqtisodiyot sharoitida axborot xavfsizligi milliy va global darajadagi eng dolzarb muammolardan biriga aylangan. An'anaviy imzo asosidagi himoya tizimlari noma'lum va murakkab kiberhujumlarga qarshi samarasiz bo'lib qolmoqda. Shu sababli, sun'iy intellekt (SI) va mashinani o'qitish texnologiyalaridan foydalangan holda real vaqt rejimida anomaliyalarni aniqlash tizimlarini yaratish zarurati tug'ilmoqda. Ushbu maqolada chuqur o'rganish algoritmlaridan foydalanib, tarmoq trafigidagi g'ayritabiiy faollikni aniqlashning yangi yondashuvi taklif etiladi.

So'nggi yillarda kiberxavfsizlik sohasida mashinani o'qitish usullarining qo'llanilishi ko'plab tadqiqotchilar tomonidan o'rganilgan. Xususan, tasniflash algoritmlari (masalan, Random Forest va Support Vector Machines) ma'lum hujum turlarini aniqlashda yuqori natija ko'rsatgan. Biroq, bu usullar katta hajmdagi dinamik ma'lumotlar oqimi bilan ishlashda va nol-kunlik (zero-day) hujumlarni aniqlashda cheklovlarga ega. Chuqur neyron tarmoqlar, xususan, avtokoderlar va rekurrent neyron tarmoqlar (RNN), vaqtinchalik bog'liqliklarni hisobga olish imkonini beradi, bu esa noaniq hujum vektorlarini aniqlashda ustunlik beradi.

Metodologiya

Tadqiqot doirasida NSL-KDD va CIC-IDS2018 ochiq ma'lumotlar bazalaridan foydalanildi. Taklif etilayotgan model ikki bosqichli arxitekturaga asoslangan. Birinchi bosqichda ma'lumotlarni oldindan qayta ishlash va normalizatsiya amalga oshirildi. Ikkinchi bosqichda Long Short-Term Memory (LSTM) tarmog'i va Avtokoder kombinatsiyasi qo'llanildi. LSTM tarmog'i tarmoq paketlaridagi vaqtinchalik ketma-ketlikni o'rganadi, avtokoder esa rekonstruksiya xatosi orqali standart holatdan chiqishlarni (anomaliyalarni) aniqlaydi. Modelning aniqligini baholash uchun Precision, Recall va F1-score metrikalari ishlatildi.

Natijalar va muhokama

O'tkazilgan eksperimentlar natijasida taklif etilgan gibrid model an'anaviy usullarga nisbatan 15 foiz yuqori aniqlikka erishdi. Xususan, DDoS hujumlarini aniqlashda F1-score ko'rsatkichi 0.94 ga yetdi. Shuningdek, model nol-kunlik hujumlarni aniqlashda ham barqaror natija ko'rsatdi, chunki u faqat ma'lum imzolarga emas, balki trafikdagi statistik og'ishlarga asoslanadi. Biroq, modelning hisoblash resurslariga talabi yuqori ekanligi aniqlandi, bu esa real vaqt rejimida katta korporativ tarmoqlarda qo'llashda optimallashtirishni talab qiladi.

Xulosa

Sun'iy intellekt texnologiyalarini kiberxavfsizlik tizimlariga integratsiya qilish zamonaviy tahdidlarga qarshi kurashishda samarali yechim hisoblanadi. Taklif etilgan LSTM va avtokoder asosidagi model anomaliyalarni aniqlash aniqligini sezilarli darajada oshiradi. Kelgusi tadqiqotlarda modelni yengillashtirish va bulutli hisoblash muhitlariga moslashtirish masalalariga e'tibor qaratish maqsadga muvofiqdir. Bu esa tizimning masshtablanuvchanligini va amaliy qo'llanilishini kengaytiradi.

Foydalanilgan adabiyotlar:

1. Smith J., Johnson A. Deep Learning for Network Intrusion Detection. Journal of Cybersecurity, 2024.

2. Rahimov B. O'zbekistonda kiberxavfsizlik holati va istiqbollari. Axborot texnologiyalari jurnali, 2025.

3. Lee S., Kim H. Hybrid AI Models in Real-time Threat Analysis. IEEE Transactions on Information Forensics, 2023.