KIBERXAVFLARNING OLDINI OLISHDA SUN‘IY INTELLEKTNING ROLI

Valiyev Davron G‘ulomboy o‘g‘li
Respublika televideniye va radio texnikumi

Annotatsiya: Mazkur maqolada zamonaviy kiberxavfsizlik tahdidlariga qarshi kurashishda sun’iy intellekt (SI) texnologiyalarining o‘rni tahlil qilinadi. Xususan, avtomatik tahdid aniqlash, anomal faoliyatni kuzatish, ma’lumotlarni himoya qilish va oldindan ogohlantirish tizimlarida SI qanday samarali yechimlar taklif qilayotgani yoritiladi. Keltirilgan real hayotiy misollar, algoritmlar asosida SI texnologiyalarining samaradorligi ochib beriladi.

Kalit so‘zlar: Sun’iy intellekt, kiberxavfsizlik, tahdidni aniqlash, mashinali o‘rganish, anomal faoliyat, xakerlik, himoya tizimi.

Kirish: Bugungi raqamli asrda kibertahdidlar soni va murakkabligi kundan-kunga ortib bormoqda. Xakerlik, zararli dasturlar, fishing, ma’lumotlar o‘g‘riligi singari holatlar kompaniyalar, davlat tashkilotlari va oddiy foydalanuvchilar uchun katta xavf tug‘dirmoqda. Oddiy antivirus yoki qo‘lda boshqariladigan xavfsizlik tizimlari bu tahdidlarga qarshi kurashishda yetarli emas. Shu nuqtada **sun’iy intellekt (SI)** texnologiyalari kiberxavfsizlikda muhim rol o‘ynay boshladi.

Asosiy qism: Sun’iy intellekt — bu kompyuter tizimlariga insoniy fikrlash, o‘rganish va muammo yechish qobiliyatlarini beruvchi texnologiya. Ushbu texnologiyaning kiberxavfsizlikdagi asosiy afzalligi — u katta hajmdagi ma’lumotlarni tez tahlil qilib, g‘ayritabiiy holatlarni aniqlay oladi. Masalan, foydalanuvchi har doim bir vaqtda tizimga kirsa, lekin birdan boshqa joydan va g‘alati vaqtda kirishga harakat qilsa, SI buni shubhali harakat sifatida ko‘rib, xavfsizlik xodimlariga xabar beradi.

Bugungi kunda ko‘plab yirik texnologik kompaniyalar o‘z tizimlarida sun’iy intellektdan foydalanmoqda. Masalan, Google o‘zining Gmail xizmatida har kuni milliardlab xabarlarni tahlil qilib, spam va fishinglarni aniqlashda SI algoritmlaridan foydalanadi. Microsoft Defender esa foydalanuvchi qurilmalarida real vaqt rejimida tahdidlarni aniqlab, ularni avtomatik tarzda bloklaydi. Bu kabi misollar SI ning xavfsizlikdagi rolini yaqqol ko‘rsatib beradi.

Bundan tashqari, sun’iy intellekt tahdidlarni nafaqat aniqlaydi, balki ularni oldindan bashorat qilishga ham yordam beradi. U ilgari yuz bergan hujumlar haqidagi ma’lumotlarni o‘rganib, kelajakda qanday tahdidlar paydo bo‘lishi mumkinligini taxmin qiladi. Bu esa kompaniyalarga oldindan chora ko‘rish imkonini beradi.

Sun’iy intellekt yordamida ishlovchi SIEM (Security Information and Event Management) tizimlari millionlab log fayllarni bir vaqtning o‘zida kuzatib, har qanday

g‘ayritabiiy harakatni aniqlay oladi. Bu tizimlar inson ko‘zi ilg‘amaydigan nozik o‘zgarishlarni ham payqaydi va xavfsizlik guruhlariga tezkor signal beradi. Aynan shu xususiyati bilan SI inson qobiliyatlarini samarali to‘ldiradi.

Shuningdek, dasturiy ta’minot yaratishda ishlatilayotgan GitHub Copilot kabi vositalar ham sun’iy intellekt asosida ishlab chiqilgan. Ular yozilayotgan kodda xavfsizlik zaifliklarini aniqlaydi va ishlab chiquvchiga xatolikni tuzatish bo‘yicha tavsiyalar beradi. Shu tarzda, dastur ishlab chiqish bosqichidanoq xavfsizlikni ta’minlash mumkin bo‘ladi.

Albatta, sun’iy intellekt insonni to‘liq almashtira olmaydi. Eng yaxshi natijalarga inson va SI o‘rtasidagi hamkorlik orqali erishiladi. SI tezlik, aniqlik va ko‘lamni ta’minlasa, inson strategik qarorlar qabul qiladi, noto‘g‘ri xulosalarni to‘g‘rilaydi va tizimni nazorat qiladi.

1. Sun’iy intellektning kiberxavfsizlikdagi afzalliklari:

Tezlik va aniqlik: Sun’iy intellekt minglab tarmoq harakatlarini bir zumda tahlil qilishi mumkin. U insondan ko‘ra tezroq tahdidlarni aniqlaydi va javob qaytaradi.

Mashinali o‘rganish: Mashinani o‘qitish algoritmlari (ML) doimiy ravishda yangi xavflarni o‘rganib, moslasha oladi. Yangi turdagi hujumlarni aniqlashda foydali.

Anomal faoliyatni kuzatish: SI foydalanuvchi odatlarini kuzatib boradi va har qanday noodatiy harakat (masalan, tunda katta hajmdagi fayllarni yuklab olish) haqida ogohlantiradi.

2. Amaliy qo‘llanmalar:

SI asosidagi antivirus dasturlar: Hozirgi antiviruslar an’anaviy ro‘yxatlarga emas, balki xatti-harakat tahliliga asoslanadi. Masalan, CrowdStrike va Darktrace kabi tizimlar real vaqt rejimida SI orqali tahdidlarni aniqlaydi.

Tarmoq xavfsizligi: SI tarmoq orqali kelayotgan ma’lumot oqimini analiz qilib, zararli trafikni ajratadi.

Fishing hujumlariga qarshi kurash: Sun’iy intellekt xat va havolalarni tahlil qilib, zararli havolalarni aniqlaydi. Gmail kabi tizimlar aynan SI orqali spam va fishing xabarlarini filtrlab beradi.

Biometrik autentifikatsiya: Yuz, barmoq izi, ovoz asosidagi autentifikatsiyada SI yordamida aniqlik oshiriladi va qalbakilashtirish ehtimoli kamaytiriladi.

3. Cheklovlar va ehtiyot choralari:

Yolg‘on ogohlantirishlar: SI ba'zida tahdid bo‘lmagan holatni ham xavf deb baholaydi.

Ma’lumotga bog‘liqlik: SI samarali ishlashi uchun ko‘p miqdorda sifatli o‘quv ma’lumotlari zarur.

Xakerlar tomonidan SI ni aldash ehtimoli: Adversarial attack — bu SI tizimini ataylab noto‘g‘ri qaror qabul qilishga undovchi usul bo‘lib, xakerlar tomonidan ishlatiladi.

Xulosa: Kiberxavfsizlikda sun’iy intellektdan foydalanish — bu zamonaviy tahdidlarga zamonaviy javobdir. Har bir tashkilot SI vositalarini o‘z xavfsizlik tizimlariga integratsiya qilish orqali nafaqat mavjud tahdidlarga qarshi kurasha oladi, balki kelajakda yuzaga keladigan xavflarga ham tayyor bo‘ladi. Biroq, SI vositalaridan foydalanishda ehtiyotkorlik, doimiy monitoring va inson nazorati muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar:

1. Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson.
2. “AI in Cybersecurity: Applications and Trends”, *Cybersecurity Ventures Report*, 2023.
3. Alan Woodward, “Artificial Intelligence and the Future of Cybersecurity”, *Journal of Cyber Policy*, 2022.
4. Darktrace official website – https://www.darktrace.com
5. IBM Security Reports – https://www.ibm.com/security/data-breach