E CONF SERIES

International Conference on Educational Discoveries and Humanities
Hosted online from Moscow, Russia
Website: econfseries.com 16th October, 2025

SUN'IY INTELLEKT ASOSIDA KIBERXAVF TAHDIDLARINI ANIQLASH VA BASHORAT QILISH TIZIMINI ISHLAB CHIQISH

Isomiddinova Zarina Sherali qizi

ANNOTATSIYA

Ushbu tezis sun'iy intellekt (SI) texnologiyalari yordamida kiberxavfsizlik tahdidlarini erta aniqlash va bashorat qilish tizimini ishlab chiqish masalalari yoritilgan. Tadqiqotda mashinaviy o'rganish, chuqur o'rganish hamda ma'lumotlarni tahlil qilish algoritmlaridan foydalangan holda tarmoqdagi zararli faoliyatni avtomatik aniqlash va xavf darajasini baholash usullari taklif etilgan. Tizim real vaqt rejimida ishlaydi hamda kiberhujumlarni oldindan prognoz qilish imkonini beradi. Natijada axborot tizimlarining xavfsizlik darajasini oshirish, zararli dasturlar va tarmoq hujumlarini tezkor bartaraf etish imkoniyatlari yaratiladi.

Kalit so'zlar: Sun'iy intellekt, kiberxavfsizlik, mashinaviy o'rganish, chuqur o'rganish, bashorat qilish, tarmoq xavfsizligi, tahdidlarni aniqlash.

Sun'iy intellekt asosida kiberxavf tahdidlarini aniqlash amaliy jihatdan bir necha real holatlar orqali tushuntiriladi. Masalan, yirik kompaniyalarning tarmog'iga har kuni millionlab foydalanuvchi kiradi va ularning har biri turli IP-manzillardan ulanadi. Oddiy kuzatuv orqali bu jarayonda g'ayritabiiy faoliyatni aniqlash qiyin, lekin sun'iy intellekt tizimi bu muammoni hal qila oladi.

U tarmoqdagi barcha kirishlarni kuzatib, foydalanuvchining odatiy xatti-harakatlarini o'rganadi. Agar foydalanuvchi odatda Toshkentdan ulanib kelayotgan bo'lsa, lekin birdan boshqa mamlakatdan tizimga kirishga urinayotgan bo'lsa, SI buni potensial kiberxavf sifatida belgilaydi va xavfsizlik xizmatiga signal beradi.

Yana bir amaliy misol sifatida elektron pochta tizimini olaylik. Har kuni minglab spam xatlar va fishing (firibgarlik) xabarlari foydalanuvchilarga yuboriladi. Sun'iy intellekt bu xatlarning matnini, yuboruvchini va havolalarini tahlil qilib, haqiqiy va soxta manbalarni ajratadi. U ilgari aniqlangan fishing xabarlaridagi so'z birikmalarini, shubhali havolalarni va rasmli ilovalarni eslab qoladi hamda yangi

kelayotgan xatlarni ular bilan solishtiradi. Natijada foydalanuvchiga zararli fayl ochilishidan oldin ogohlantirish yuboriladi.

Korxonalarda esa sun'iy intellekt xavfsizlik kameralaridan, kirish nazorat tizimlaridan va server loglaridan olingan ma'lumotlarni birlashtirib, kiberxavfga olib kelishi mumkin bo'lgan noan'anaviy harakatlarni aniqlaydi. Misol uchun, xodim odatda faqat ish vaqtida serverga kiradi, lekin bir kechasi tizimga bir necha marta kirishga uringan bo'lsa, SI bu holatni avtomatik tarzda xavfli sifatida belgilaydi va administratorga xabar beradi.

Shuningdek, sun'iy intellekt tarmoq trafikidagi o'zgarishlarni real vaqt rejimida kuzatadi. Agar ma'lum bir IP-manzildan juda ko'p so'rovlar yuborilayotgan bo'lsa, bu xizmatni ishdan chiqarishga qaratilgan DDoS hujumi bo'lishi mumkin. Tizim bunday holatni aniqlab, avtomatik tarzda u manzilni bloklaydi yoki so'rovlar oqimini muvozanatlashtiradi.

Kreativ yondashuv sifatida, ayrim kompaniyalar sun'iy intellektga "kiberxavf detektivi" rolini berishadi. U tarmoqda harakatlanayotgan barcha ma'lumotlarni kuzatadi, ular orasida shubhali "izlar"ni topadi va hujumni oldindan taxmin qiladi. Masalan, u foydalanuvchilarning parolni kiritishdagi xatti-harakatlarini ham kuzatib, noto'g'ri kiritishlar soni, tezligi va kirish vaqti orqali parolni buzishga urinayotgan bot yoki insonni farqlay oladi.

Bunday amaliy yondashuvlar sun'iy intellektning nafaqat reaktiv, balki proaktiv (ya'ni oldindan ogohlantiruvchi) tizim sifatida ishlashini ta'minlaydi. Natijada kiberxavflarni aniqlash, tahlil qilish va bartaraf etish jarayoni inson aralashuvisiz tez, aniq va samarali amalga oshiriladi.

Sun'iy intellekt asosida kiberxavf tahdidlarini aniqlash va bashorat qilish tizimini ishlab chiqish amaliy jihatdan quyidagicha tasavvur qilinadi:

Kompyuter tarmog'ida maxsus AI xavfsizlik paneli yaratiladi. Bu panel real vaqt rejimida barcha foydalanuvchi kirishlarini, tarmoq trafigini va server loglarini kuzatadi. Masalan, tizimga o'rnatilgan neyrontarmoq modeli har bir foydalanuvchining xatti-harakatlaridan o'rganadi: kim, qachon, qaysi faylga kirgan, qanday qurilmadan foydalangan. Shundan so'ng u "normal" faoliyat namunalarini shakllantiradi.

Bir kuni tizim bitta foydalanuvchi odatda kuniga faqat 10 megabayt fayl yuklaydiganini kuzatgan bo‘lsa, ammo birdan yuzlab fayllarni yuklab, tashqi manzilga yuborayotganini aniqlaydi. AI bu holatni real vaqt rejimida aniqlaydi va “data leak” (ma’lumot sizib chiqishi) ehtimolini hisoblab chiqadi. Natijada tizim avtomatik ravishda bu foydalanuvchini vaqtincha bloklaydi va xavfsizlik xodimiga xabar beradi.

Keyingi bosqichda bashorat qilish mexanizmi ishga tushadi. Tizim o‘tgan oylar davomida to‘plangan barcha kiberfaoliyat ma’lumotlarini tahlil qiladi masalan, qaysi kunlarda hujumlar ko‘p bo‘lgan, qaysi IP-manzillar ko‘p tarmoqni tekshirgan, qaysi fayllarda zararli kodlar aniqlangan. Ushbu tarixiy ma’lumot asosida AI algoritmi kelgusi haftada qaysi vaqtda yoki qaysi yo‘nalishda kiberhujum bo‘lish ehtimolini bashorat qiladi.

Amaliy jihatdan bu jarayon grafik interfeysda quyidagicha ko‘rinadi: ekran markazida real vaqtli tarmoq xaritasi paydo bo‘ladi. Har bir server, foydalanuvchi va IP-manzil tugunlar shaklida belgilanadi. Agar AI shubhali faoliyatni sezsa, u tugunni qizil rangda yoritadi. Yon panelda esa “tahdid turi fishing, DDoS, malware” kabi bashoratlar chiqadi va “bashorat aniqligi: 92%” kabi ko‘rsatkichlar aks etadi.

Bundan tashqari, tizimda self-learning (o‘zi o‘rganish) moduli bo‘ladi. Har safar yangi kiberhujum ro‘y bersa, AI bu holatdan o‘rganadi. Masalan, avval ma’lum bo‘lmagan zararli fayl turlari aniqlansa, tizim uning xususiyatlarini tahlil qilib, kelajakda shu turdagi hujumlarni erta bosqichda aniqlashni o‘rganadi.

Yana bir amaliy misol tizim serverlararo muloqotlarni kuzatadi. Agar u birdan tarmoqda mavjud bo‘lmagan, “soxta” server bilan aloqa o‘rnatilganini sezsa, darhol uni aniqlaydi, keyin esa bashorat modeli orqali shu soxta manzil orqali kelajakda yana shunday hujumlar bo‘lish ehtimolini hisoblaydi. Shu tariqa tizim faqat himoya qilmaydi, balki kiberxavflarning oldini oladi.

Bunday amaliy tizim natijasida korxonalar va tashkilotlar o‘z tarmoqlarida kiberxavf belgilari paydo bo‘lishini nafaqat kuzatadi, balki ular sodir bo‘lishidan oldinroq chora ko‘rish imkoniga ega bo‘ladi.

XULOSA

Xulosa qilib aytganda, sun’iy intellekt asosida kiberxavf tahdidlarini aniqlash va bashorat qilish tizimini ishlab chiqish zamonaviy axborot xavfsizligini ta’minlashda eng samarali yondashuvlardan biridir. Amaliy misollar orqali ko‘rish mumkinki, bunday tizimlar real vaqt rejimida tarmoqdagi g‘ayritabiiy harakatlarni aniqlay oladi, ma’lumotlar oqimini tahlil qiladi va hujumlar yuz berishidan oldin ogohlantirish beradi. Sun’iy intellekt texnologiyalari, xususan mashinaviy va chuqur o‘rganish algoritmlari yordamida tizim o‘z-o‘zini yangilab boradi, yangi tahdid turlarini o‘rganadi va ularni bartaraf etish strategiyasini taklif qiladi. Natijada inson aralashuvisiz ishlaydigan, o‘zini mustaqil himoya qila oladigan va xavfsizlik darajasini doimiy oshirib boradigan aqlli kiberxavfsizlik muhitini yaratish imkoniyati paydo bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Temirbekov Sayfiddin Farxodjon. Sun’iy intellekt yordamida avtomatlashtirilgan hujumlarni qaytarish va oldini olish. Ilmiy tadqiqotlar va ularning yechimlari jurnali, 2024. worldlyjournals.com
2. Tursunbek Sadriddinovich Jalolov. Sun’iy intellekt va kiberxavfsizlik yordamida tahdidlarni aniqlashda AI roli. Pedagogik Tadqiqotlar Jurnali, 2024. wosjournals.com
3. Azizbek Xaitbayev Pirnazarovich. Kiberxavfsizlikda sun’iy intellect. Modern Education and Development jurnali, 2024. ilmiyxabarlar.uz
4. Husanova Gulnozaxon Orifjon qizi. Sun’iy intellekt, kiberxavfsizlik va axborot texnologiyalar: nazariya, amaliyot va XXI asr chaqiriqlari. TADQIQOTLAR jahon ilmiy-metodik jurnali, 2025. scientific-jl.com