AI YORDAMIDA LOG TAHLILINI AVTOMATLASHTIRISH

Musurmonov Behruz Farhodjon o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, talabasi

Annotatsiya: *Ushbu maqolada sun’iy intellekt (AI) texnologiyalaridan foydalangan holda log tahlilini avtomatlashtirish masalasi keng yoritilgan. Axborot tizimlarida har kuni hosil bo‘ladigan millionlab log yozuvlarini qo‘lda yoki an’anaviy usullar bilan tahlil qilish tobora murakkablashib bormoqda. Shu bois, log ma’lumotlaridagi anomaliyalarni aniqlash, xavfsizlik hodisalarini erta bosqichda kuzatish hamda tizim faoliyatini real vaqt rejimida baholash uchun AI asosidagi yondashuvlar muhim ahamiyat kasb etmoqda. Maqolada mashinaviy o‘rganish (ML), tabiiy tilni qayta ishlash (NLP) va chuqur o‘rganish (DL) usullarining log tahlilidagi amaliy qo‘llanilishi tahlil qilinadi. Shuningdek, Wazuh, SIEM va XDR tizimlari misolida AI yordamida tahlil jarayonini optimallashtirish usullari keltirilgan. Tadqiqot natijalari shuni ko‘rsatadiki, sun’iy intellekt asosidagi log tahlil tizimlari xavfsizlikni oshirish, inson omilini kamaytirish hamda tahlil tezligini bir necha baravar ko‘paytirishga yordam beradi.*

Kalit so’zlar: *Sun’iy intellekt (AI), Mashinani o‘rganish (ML),Tabiiy tilni qayta ishlash (NLP), Log tahlili, Anomaliya aniqlash, Kiberxavfsizlik, Avtomatlashtirish, SIEM (Security Information and Event Management), XDR (Extended Detection and Response), Tahdid ovlash (Threat Hunting).*

KIRISH

Bugungi kunda axborot tizimlari va ilovalari juda ko‘p hajmdagi log ma’lumotlarini ishlab chiqadi. Global darajada yaratilayotgan ma’lumotlar miqdori 2025-yilgacha 181 zettabaytgacha etishi prognoz qilinmoqda. Log ma’lumotlari kompyuter tizimi, tarmog‘i yoki ilovada sodir bo‘lgan voqealar haqidagi vaqt belgili batafsil yozuvlarni o‘z ichiga oladi. Ushbu yozuvlarni tahlil qilish tizimning ish faoliyati, nosozliklar va kiberxavfsizlik tahdidlarini aniqlashda muhim ahamiyat kasb etadi. Masalan, IBM ma’lumotlariga ko‘ra, so‘nggi besh yilda korxona darajasidagi log ma’lumotlarini tahlil qilish hajmi yillik 250% ga oshgan. Shu bois log tahlilining avtomatlashtirilishi va unga sun’iy intellekt joriy etilishi dolzarb vazifa sifatida yuzaga kelmoqda. An’anaviy usullarda logni qo‘lda tekshirish katta hajmdagi va turlicha formatdagi ma’lumotlar bilan ishlashda samarasiz bo‘lib, xatolik ehtimolini oshiradi. Shu sababli ko‘plab tashkilotlar AI yordamida loglarni yig‘ish, tozalash, indeksatsiya va tahlil qilish jarayonlarini avtomatlashtirish orqali vaqti-vaqti bilan yuz beradigan muammolarni erta aniqlab kelmoqda.

ASOSIY QISM

Log tahlilining roli va murakkabligi

Loglar tizimlarning kunlik ish faoliyatini yozib boruvchi elektron kundaliklar hisoblanadi. Ular yordamida administrator va xavfsizlik bo‘limlari tizimlarda sodir bo‘layotgan hodisalarni kuzatib boradi, nosozliklarni aniqlaydi va salbiy hodisalarning oldini oladi. Biroq, hozirgi kunda loglar soni va xilma-xilligi juda yuqori darajaga yetgan. Log formatlari birhil emasligi, ularning tarkibi va sababi har xil bo‘lishi tufayli avtomatlashtirilmagan tahlil murakkablashadi. Bundan tashqari, tizimlardagi anomaliyali hodisalar odatda kam uchraydigan va turlicha tus olganligi sababli, ularni aniqlash uchun oddiy statistik qoidalarga tayanish yetarli bo‘lmay qoladi. Misol uchun, an’anaviy usullar ko‘p miqdordagi log ma’lumotlaridagi nozik naqshlarni yuqori aniqlikda aniqlash imkoniyatini sekinlashtiradi yoki umuman bajara olmaydi. Shu bois log tahlili zamonaviy IT muhitida murakkab va mehnat talab qiluvchi jarayon hisoblanadi.

An’anaviy va AI asosidagi yondashuvlarning taqqoslanishi

An’anaviy log tahlili ko‘pincha ma’lum qoidalar va filtr asosida amalga oshiriladi. Masalan, vaqt oralig‘i, xato kodlari yoki oldindan belgilangan kalit so‘zlarga asosan log yozuvlari filtrlab olinadi. Biroq bunday yondashuv yangi yoki noaniq tahdidlarni aniqlashda, shuningdek bir vaqtning o‘zida katta hajmdagi logni qayta ishlashda samarali emas. IBM ta’kidiga ko‘ra, an’anaviy log tahlili vositalari ma’lumotlar oqimining ekspansiv o‘sishiga javob bera olmaydi. Shu bois, sun’iy intellekt va mashinani o‘rganish asboblari log tahlilini avtomatlashtirishga kirib kelmoqda: ular katta hajmdagi ma’lumotni tezkor qayta ishlaydi va murakkab naqshlarni aniqlaydi. Masalan, AI algoritmlari inson tahlilchilariga bir necha kun yoki oylar talab qilgan anomaliya aniqlash va sabablashni avtomatlashtirib bajaradi.

EdgeDelta ma’lumotlariga ko‘ra, log tahlilida mashinani o‘rganishning ikkita asosiy usuli mavjud: nazoratli (supervised) va nazoratsiz (unsupervised) o‘rganish. Nazoratli usulda model aniqlangan namunalarga tayangan holda o‘qitiladi, nazoratsizda esa model o‘zi ma’lumotlardagi naqshlarni izlab topadi. AI vositalari bu yondashuvlarni birlashtirib, avvalo oddiy quyidagilardan iborat bo‘lgan jarayonni tezlashtiradi: loglarni yig‘ish, normalizatsiya qilish va indekslash, so‘ng model yordamida nazariy normal holatga nisbatan anomaliyalarni qidirish. Bunda misol uchun Log file tahliliga tayyorlangan modellarga LLPlatari kiritilib, ular log satrlaridagi matnli tafsilotlar asosida malumotlarning semantik va sekvential bog‘liqligini hisobga oladi. Aslida Transformer arxitekturasi kabi ilg‘or NLP modellarini (masalan, GPT) log anomaliyalarini aniqlashda qo‘llash hali ilmiy tadqiqotlarda o‘z samarasini ko‘rsatmoqda.

AI texnologiyalarining amaliy imkoniyatlari (ML, NLP, anomal-liya aniqlash)

AI yondashuvlari log ma’lumotlari ustida turli texnologiyalarni birlashtiradi. Mashinani o‘rganish (ML) algoritmlari – qaror daraxtlari, SVM, sinfga ajratish (clustering) yoki neyron tarmoqlar bo‘lsin – logdan xususiyatlar olish va ularni tahlil qilish uchun ishlatiladi. Masalan, anomalya aniqlash bo‘yicha oddiy statistika, klasterlash va chuqur o‘rganish metodlari qo‘llanadi; kelib tushayotgan loglar normal holatdan chetga chiqqan holda klassifikatsiya qilinadi. Sun’iy neyron tarmoqlar va vaqt ketma-ketlik modellarini (RNN, LSTM) log voqealarining vaqtli o‘zgarishini o‘rganish va oldingi hodisalarga asoslanib voqealarni bashorat qilish uchun keng ishlatishadi. Yana bir soha – tabiiy tilni qayta ishlash (NLP). Log

yozuvlari ko‘pincha erkin matnli tuzilmada bo‘lgani uchun, NLP usullari bu yozuvlardan ma’no chiqarish va strukturali ma’lumotga aylantirishga yordam beradi. Shuningdek, transformer asosidagi modellar (BERT, LogBERT, GPT va boshqalar) log matnlarini tushunib, anomaliyalarni aniqlash va log hodisalarini generatsiya qilish kabi vazifalarda qo‘llanmoqda.

Qo‘shimcha ravishda, anomaliya aniqlash sohasida AI juda keng qo‘llaniladi. Splunk va boshqa platformalarning ma’lumotlariga ko‘ra, anomaliya aniqlash haqiqiy muammolarni oldini olish uchun muhimdir. Masalan, ma’lum targ‘ibotlar ko‘rsatishicha, anomaliyalarni aniqlash tizimlari tarmoq kirishini real vaqtda kuzatish, xavfsizlik xurujlari yoki texnik nosozliklarni erta qidirishga imkon beradi. Ular statistik, mashinani o‘rganish va chuqur o‘rganish kabi texnikalarni birlashtiradi, natijada qoidalar asosidagi tizimlarga nisbatan aniqroq natija beradi. Anomaliyalar tiplariga kelsak, bir log yozuvi (point anomaly), vaziyatga bog‘liq to‘plam (contextual) yoki bir nechta baytlar guruhining to‘planishi (collective anomaly) kabi turlari mavjudligi tushuntiriladi.

Real hayotdagi qo‘llanilish misollari (Wazuh, SIEM, XDR)

Real sharoitda sun’iy intellektli log tahlil tizimlari turli mahsulot va yechimlarda o‘z aksini topmoqda. Masalan, Wazuh – bu ochiq manbali platforma bo‘lib, u XDR va SIEM imkoniyatlarini birlashtiradi. Wazuh loglarni markazlashtirib yig‘adi va ular ustida tahdid ovlashni avtomatlashtiradi. Sun’iy intellekt Wazuhga kiritilganida tahdidlarni qidirish jarayonlari sezilarli tezlashadi: katta hajmdagi xavfsizlik ma’lumotlarini yuqori tezlikda qayta ishlash, kichik naqsh va anomaliyalarni aniqlash kabi afzalliklar qo‘lga kiradi. Shu bilan birga, klassik SIEM (Security Information and Event Management) tizimlari turli manbalardan – serverlar, ilovalar, tarmoq qurilmalari va xavfsizlik vositalaridan – keluvchi log ma’lumotlarini markazlashtiradi va ularni real vaqt rejimida tahlil qiladi. SIEM vositalari hodisalarni korrelyatsiya qilish va oldindan belgilangan qoidalar bo‘yicha alertlar jo‘natish orqali jamoalarga xavfli hodisalarni erta aniqlash imkonini yaratadi. XDR (Extended Detection and Response) platformalari esa SIEM’ning an’anaviy log yig‘ishni to‘ldirib, kengaytirilgan ma’lumot tahliliga yo‘naltirilgan. XDR endpoint, tarmoq trafik va bulut muhitlari kabi ko‘p qatlamli telemetriya ma’lumotlarini birlashtirib, xavfsizlik holatini yanada kengroq doirada kuzatadi va ilg‘or tahlil metodlari yordamida yangi tahdidlarni aniqlaydi.

AI asosidagi tizim arxitekturasi va samaradorlik tahlili

AI yordamida log tahlilini tashkil etuvchi tizimlar odatda bir necha bosqichdan iborat bo‘ladi. Avvalo, log ma’lumotlari turli manbalardan (tarmoqlar, serverlar, ilovalar) avtomatik ravishda yig‘iladi. IBM Think nashrida aytilishicha, bu bosqichda sun’iy intellekt log ma’lumotlarini yig‘ish jarayonini avtomatlashtiradi va ularni markazlashtirilgan muhitga jo‘natadi. So‘ngra Data Processing bosqichi bo‘lib, u yerda AI loglarni indeksatsiya va normalizatsiya yordamida tozalaydi, ya’ni parsing orqali ularni vaqt, manba va hodisa turiga qarab kategoriyalarga ajratadi. Ushbu bosqich loglarni bir xil shaklga keltirib, noz‘il ma’lumotlardan xoli, tadqiqotchilar uchun tushunarli ko‘rinishga keltiradi. Keyingi Data Analysis bosqichida logdan olingan tuzilgan ma’lumotlar ustida tahlil o'tkaziladi. Bu yerda AI/ML modullari anomaliya aniqlash va naqsh tanib olish qobiliyatlaridan foydalangan holda

tizim xatti-harakatlarini baholaydi. Misol uchun, ilg‘or AI algoritmi normal holatni o‘rganib, undan farq qiluvchi holatlarni belgilaydi va ogohlantirish beradi. Oxirgi bosqich — Data Visualization —da esa tahlil natijalari boshqaruv paneli orqali vizual tarzda namoyish etiladi, bu tizimning real vaqtdagi holatini tushunishni soddalashtiradi.

Bunday arxitektura samaradorligi ko‘plab amaliy namunalar bilan tasdiqlangan. Tashkilotlar sun’iy intellektli log tahlili yechimlarini joriy qilish orqali jiddiy tejashlarga erishmoqda. Masalan, IBM ma’lumotiga ko‘ra, kiberxavfsizlikda AI va avtomatlashtirishni keng qo‘llagan tashkilotlar o‘rtacha 2,2 million AQSH dollari miqdorida xarajatlarni kamaytirdi. Ushbu natija avtomatlashtirishning ITOps va xavfsizlik samaradorligini sezilarli darajada oshirganini ko‘rsatadi.

XULOSA

Xulosa qilib aytganda, sun’iy intellekt yordamida log tahlilini avtomatlashtirish zamonaviy axborot tizimlarida muhim o‘rin tutadi. Bunday yondashuv log ma’lumotlarini real vaqtda qayta ishlash, tizimdagi nosozliklarni va tahdidlarni aniqlash jarayonini jadal va yuqori aniqlik bilan bajarish imkonini beradi. Misol uchun, Wazuh platformasida AI integratsiyasi xavfsizlik ma’lumotlarini avtomatik tahlil qilish orqali tahlilchilar e’tiborini asosiy muammolarga qaratishga yordam beradi. Kelgusida esa gen AI (masalan, oldindan o‘qitilgan LLM) va agentli AI vositalarining rivojlanishi log tahlilini yanada avtonom va aqlli qiladi. Xulosa qilib aytganda, AI asosidagi log tahlili yondashuvlari xavfsizlik operatsiyalarini optimallashtiradi hamda tashkilotlar uchun yangi imkoniyatlar ochadi, ular esa kelajakda ham rivojlanishni davom ettiradi.

Xulosa qilib aytganda, axborot xavfsizligini ta’minlash tizimli va kompleks choralar talab qiladi. Zamonaviy texnologiyalar (AI/ML asosidagi tahdidlarni aniqlash, Zero Trust, XDR kabi) va xalqaro xavfsizlik yondashuvlari birgalikda korxona ma’lumotlarini samarali himoya qilish imkonini beradi.

Standartlar bo‘yicha ISMSni joriy etish esa tashkilotlarga xavf-xatarlarni sistematik boshqarish, uzluksiz audit va doimiy takomillashtirishni olib borishga yordam beradi.

ADABIYOTLAR RO’YXATI:

1. Mesh Flinders, Ian Smalley. “What is log analysis with AI?” IBM Think, 2024

2. Farouk Musa. “Leveraging artificial intelligence for threat hunting in Wazuh.” Wazuh Blog, 13 июнь 2025

3. Wazuh Documentation. “Getting started with Wazuh.” Wazuh docs, 2024

4. “What Is Security Information and Event Management (SIEM)? 7 Pillars and 13 Core Features.” Exabeam Explainers, 2025

5. Palo Alto Networks. “What is the Difference Between XDR vs. SIEM?” Cyberpedia, 2023

6. Y. Zhang, et al. “A Novel GPT-Based Framework for Anomaly Detection in System Logs.” arXiv preprint, 2024

7. Xu X. va boshq. “Practitioners’ Expectations on Log Anomaly Detection.” arXiv preprint, 2024

8. Weian Li va boshq. “System log anomaly detection based on contrastive learning and retrieval augmented.” Scientific Reports, 2025

9. Edge Delta Team. “Unveiling the Dynamic Shift: Log Analysis Evolution Through AI and ML.” Edge Delta Blog, 13 mart 2024

10. LogicMonitor Blog. “What is log file analysis? Overview and best practices.” LogicMonitor, 2024