SUN'IY INTELLEKT ASOSIDA BULUTLI TEXNOLOGIYALARDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI

Abrayev Azamat Kamoliddinovich
Qarshi davlat texnika universiteti Raqamli texnologiyalar va sun'iy intellekt fakulteti "Kompyuter tizimlarining dasturiy va texnik ta'minoti" kafedrasi assistenti
https://doi.org/10.5281/zenodo.23660434

Annotatsiya

Mazkur tezisda bulutli hisoblash texnologiyalarida ma'lumotlar xavfsizligini ta'minlashda sun'iy intellekt texnologiyalaridan foydalanish imkoniyatlari tahlil qilinadi. Bulutli infratuzilmaning rivojlanishi, ma'lumotlarni saqlash va qayta ishlash jarayonlarida yuzaga keladigan kiberxavfsizlik tahdidlari hamda ularni aniqlash usullari yoritiladi. Shuningdek, sun'iy intellekt asosida ishlaydigan monitoring tizimlari, anomaliyalarni aniqlash algoritmlari, avtomatik tahdid tahlili va foydalanuvchilar faoliyatini nazorat qilish mexanizmlarining ahamiyati ko'rib chiqiladi. Tahlil natijalari sun'iy intellekt bulutli muhitda xavfsizlik hodisalarini tezkor aniqlash va ularga javob berish imkoniyatlarini kengaytirishini ko'rsatadi. Shu bilan birga, bunday tizimlardan samarali foydalanish uchun ma'lumotlar maxfiyligi, algoritmlar ishonchliligi va inson nazoratini ta'minlash muhim hisoblanadi.

Kalit so'zlar: sun'iy intellekt, bulutli hisoblash, ma'lumotlar xavfsizligi, kiberxavfsizlik, mashinaviy o'qitish, anomaliyalarni aniqlash, shifrlash, Big Data, raqamli transformatsiya.

Kirish

Raqamli iqtisodiyotning rivojlanishi natijasida axborot resurslarini xavfsiz saqlash, qayta ishlash va uzatish masalalari dolzarb ahamiyat kasb etmoqda. Bugungi kunda ta'lim muassasalari, korxonalar, banklar va davlat tashkilotlari o'z faoliyatida katta hajmdagi ma'lumotlardan foydalanmoqda. Ushbu ma'lumotlarni samarali boshqarish uchun bulutli hisoblash texnologiyalari keng qo'llanilmoqda.

Bulutli hisoblash foydalanuvchilarga internet orqali masofaviy serverlar, saqlash resurslari va dasturiy xizmatlardan foydalanish imkonini beradi. Amazon Web Services, Microsoft Azure va Google Cloud kabi platformalar turli tashkilotlarning axborot infratuzilmasini rivojlantirishda muhim o'rin tutadi. Biroq bulutli muhitda ma'lumotlarning markazlashtirilgan holda saqlanishi ruxsatsiz kirish, zararli dasturlar, fishing va boshqa kiberhujumlar xavfini ham yuzaga keltiradi.

An'anaviy himoya vositalari ko'pincha oldindan ma'lum bo'lgan tahdidlarni aniqlashga asoslanadi. Zamonaviy kiberhujumlarning murakkablashishi esa xavfsizlik tizimlaridan katta hajmdagi axborotlarni tahlil qilish, noodatiy faoliyatni aniqlash va tahdidlarga tezkor javob berishni talab etadi. Shu nuqtayi nazardan, sun'iy intellekt va mashinaviy o'qitish algoritmlarini bulutli xavfsizlik tizimlariga joriy etish muhim ilmiy-amaliy yo'nalish hisoblanadi.

Bulutli texnologiyalar va sun'iy intellektning o'zaro integratsiyasi

Bulutli hisoblash texnologiyalari odatda IaaS (Infrastructure as a Service), PaaS (Platform as a Service) va SaaS (Software as a Service) xizmat modellariga ajratiladi. IaaS virtual serverlar va tarmoq resurslarini, PaaS dastur ishlab chiqish muhitini, SaaS esa internet orqali foydalaniladigan tayyor dasturiy xizmatlarni taqdim etadi.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Sun'iy intellekt ushbu modellarda ma'lumotlarni tahlil qilish, xizmatlar samaradorligini oshirish va xavfsizlik jarayonlarini avtomatlashtirish uchun qo'llanilishi mumkin. Masalan, mashinaviy o'qitish algoritmlari foydalanuvchilarning odatiy faoliyatini o'rganib, undan keskin farq qiluvchi harakatlarni aniqlashga yordam beradi.

Bulutli muhitda sun'iy intellektdan foydalanishning asosiy afzalliklaridan biri katta hajmdagi ma'lumotlarni tezkor qayta ishlash imkoniyatidir. Tizim serverlarga kirishlar, tarmoq trafigi va ilovalar jurnallarini tahlil qilib, shubhali holatlar yuzasidan ogohlantirish yaratishi mumkin. Bunda algoritmlarning samaradorligi ma'lumotlar sifati, modelning to'g'ri sozlanishi va xavfsizlik siyosatiga bog'liq bo'ladi.

Sun'iy intellekt yordamida kiberxavfsizlik tahdidlarini aniqlash

Bulutli infratuzilmada uchraydigan asosiy tahdidlarga ruxsatsiz kirish, hisob ma'lumotlarining o'g'irlanishi, DDoS hujumlari, zararli dasturlar va ma'lumotlarning yo'qolishi kiradi. Sun'iy intellekt ushbu tahdidlarni aniqlashda bir nechta yondashuvlardan foydalanishi mumkin.

Birinchidan, anomaliyalarni aniqlash algoritmlari tizimdagi odatiy faoliyatdan farq qiluvchi holatlarni topadi. Masalan, foydalanuvchining qisqa vaqt ichida juda ko'p marta tizimga kirishga urinishi yoki odatdagidan keskin farq qiluvchi ma'lumotlar hajmini yuklab olishi qo'shimcha tekshiruv uchun signal bo'lishi mumkin.

Ikkinchidan, mashinaviy o'qitish usullari tarmoq trafigi va xavfsizlik jurnallaridagi takrorlanuvchi belgilarni tahlil qilish orqali ehtimoliy hujumlarni aniqlashga yordam beradi.

Uchinchidan, tabiiy tilni qayta ishlash texnologiyalari xavfsizlik jurnallari va hodisalar haqidagi matnli hisobotlarni tahlil qilishda qo'llanilishi mumkin.

Shuni ta'kidlash kerakki, sun'iy intellekt barcha kiberhujumlarni mustaqil va xatosiz aniqlay olmaydi. Noto'g'ri ogohlantirishlar, yangi hujum turlari va algoritmlarga qarshi amalga oshiriladigan ta'sirlar tizim samaradorligini pasaytirishi mumkin. Shu sababli sun'iy intellektni an'anaviy xavfsizlik vositalari, ekspert tahlili va inson nazorati bilan birgalikda qo'llash maqsadga muvofiqdir.

Ma'lumotlar xavfsizligini ta'minlashning zamonaviy usullari

Bulutli muhitda ma'lumotlarni himoyalash uchun texnologik va tashkiliy choralar kompleks ravishda amalga oshirilishi lozim. Eng muhim usullardan biri — ma'lumotlarni saqlash va uzatish jarayonida shifrlashdan foydalanishdir. Shifrlash axborotning ruxsatsiz shaxslar tomonidan o'qilishini cheklaydi. Ko'p faktorli autentifikatsiya foydalanuvchi shaxsini bir nechta mustaqil omil yordamida tekshirish imkonini beradi. Kirish huquqlarini cheklash tamoyili esa har bir foydalanuvchiga faqat o'z vazifasini bajarishi uchun zarur bo'lgan resurslardan foydalanishga ruxsat berishni nazarda tutadi.

Sun'iy intellekt asosidagi monitoring tizimlari ushbu himoya mexanizmlarini to'ldiradi. Ular foydalanuvchilar faoliyatidagi o'zgarishlarni kuzatishi, shubhali hodisalarni ustuvorlik bo'yicha ajratishi va mas'ul mutaxassislarga xabar berishi mumkin. Ayrim hollarda, oldindan belgilangan qoidalar asosida shubhali seansni vaqtincha cheklash yoki qo'shimcha autentifikatsiyani talab qilish ham mumkin. Bundan tashqari, zaxira nusxalarini muntazam yaratish, dasturiy ta'minotni yangilab borish va xavfsizlik auditini o'tkazish ma'lumotlarning yaxlitligi hamda xizmatlarning uzluksizligini ta'minlashga xizmat qiladi. Sun'iy intellektga asoslangan tizimlarning o'zi ham himoyalanishi, ular foydalanadigan ma'lumotlar esa maxfiylik talablariga muvofiq boshqarilishi kerak.

Sun'iy intellekt asosidagi bulutli xavfsizlikning istiqbollari

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Kelajakda bulutli hisoblash, sun'iy intellekt, katta ma'lumotlar va Internet of Things texnologiyalarining integratsiyasi yanada kengayishi kutiladi. Bunday integratsiya ko'plab qurilmalar va axborot tizimlaridan keladigan ma'lumotlarni birgalikda tahlil qilish imkonini beradi.

Zero Trust xavfsizlik modeli ham ushbu jarayonda muhim ahamiyatga ega. Mazkur yondashuvda foydalanuvchi yoki qurilmaga faqat tarmoq ichida joylashgani uchun ishonch bildirilmaydi; har bir kirish so'rovi belgilangan xavfsizlik talablari asosida tekshiriladi. Sun'iy intellekt ushbu tekshiruvlarda xavf darajasini baholash va noodatiy faoliyatni aniqlashga ko'maklashishi mumkin. Shu bilan birga, sun'iy intellektdan foydalanishda shaxsiy ma'lumotlarning maxfiyligi, algoritmlarning shaffofligi va qarorlarning izohlanishi masalalariga e'tibor berish zarur. Kelgusida xavfsizlik tizimlarining samaradorligi nafaqat tahdidlarni aniqlash tezligi, balki noto'g'ri qarorlarni kamaytirish va inson nazoratini saqlash bilan ham belgilanadi.

Xulosa

Xulosa qilib aytganda, bulutli hisoblash texnologiyalari zamonaviy raqamli infratuzilmaning muhim tarkibiy qismi bo'lib, ularda ma'lumotlar xavfsizligini ta'minlash doimiy takomillashtirishni talab qiladi. Sun'iy intellekt va mashinaviy o'qitish algoritmlari xavfsizlik hodisalarini tahlil qilish, noodatiy faoliyatni aniqlash va tahdidlarga javob berish jarayonlarini takomillashtirish imkoniyatiga ega. Biroq sun'iy intellektni joriy etishning o'zi to'liq xavfsizlikni kafolatlamaydi. Ishonchli himoyani shakllantirish uchun shifrlash, ko'p faktorli autentifikatsiya, kirish huquqlarini boshqarish, zaxira nusxalash va muntazam audit kabi mexanizmlardan kompleks foydalanish lozim. Shuningdek, algoritmlarning natijalarini inson tomonidan nazorat qilish va ma'lumotlar maxfiyligini ta'minlash muhimdir.

Demak, sun'iy intellekt va bulutli texnologiyalar integratsiyasi kiberxavfsizlikni rivojlantirishning istiqbolli yo'nalishlaridan biri hisoblanadi. Ushbu texnologiyalarni oqilona va mas'uliyatli qo'llash raqamli xizmatlarning ishonchliligi hamda barqarorligini oshirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Mell P., Grance T. The NIST Definition of Cloud Computing. NIST Special Publication 800-145, 2011.
2. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson.
3. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1, 2023.
4. National Institute of Standards and Technology. Zero Trust Architecture. NIST Special Publication 800-207, 2020.
5. National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024.
6. Amazon Web Services, Microsoft Azure va Google Cloud platformalarining bulutli xavfsizlik bo'yicha rasmiy texnik hujjatlari.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.