MASHINANI O‘QITISH USULLARI VA UNING NOQONUNIY MAYNING FAOLIYATINI ANIQLASH SOHASIGA TATBIQI

Risqaliyev Jaxongir Dadajon-o‘g‘li
Ichki ishlar vazirligi Malaka oshirish instituti katta o‘qituvchisi
E-mail: jaxongir.tmi93@gmail.com

Annotatsiya. Ushbu maqolada mashinani o‘qitish (Machine Learning) usullari yordamida noqonuniy mayning faoliyatini aniqlash sohasida qo‘llanilish imkoniyatlari tahlil qilinadi. Mayning faoliyatining texnik xususiyatlari, uning noqonuniy shakllarini aniqlashdagi muammolar hamda mashinani o‘qitish usullarining afzalliklari yoritilgan. Maqolada klassifikatsiya va anomaliyani aniqlash algoritmlari asosida umumiy model konsepsiyasi taklif etiladi. Taklif etilgan yondashuv kiberxavfsizlik tizimlarida, xususan, noqonuniy mayning faoliyatini erta aniqlashda qo‘llanishi mumkin.

Kalit so‘zlar: mashinani o‘qitish, mayning faoliyati, kiberxavfsizlik, sun’iy intellekt.

Аннотация. В данной статье анализируется потенциальное применение методов машинного обучения при выявлении незаконной горной деятельности. Выделяются технические характеристики горных работ, проблемы выявления их незаконных форм, преимущества машинного обучения. В работе предложена общая концепция модели, основанная на алгоритмах классификации и обнаружения аномалий. Предлагаемый подход может быть реализован в системах кибербезопасности, особенно для раннего выявления незаконной деятельности по майнингу.

Ключевые слова: машинное обучение, майнинговая деятельность, кибербезопасность, искусственный интеллект.

Abstract. This article analyzes the potential applications of machine learning methods in detecting illegal mining activities. The technical characteristics of mining operations, challenges in identifying their illegal forms, and the advantages of machine learning techniques are highlighted. The paper proposes a general model concept based on classification and anomaly detection algorithms. The suggested approach can be implemented in cybersecurity systems, particularly for the early detection of illegal mining activities.

Keywords: Machine learning, mining activities, cybersecurity, artificial intelligence.

Kirish.

So‘nggi yillarda kripto-aktivlarning ommalashuvi bilan bir qatorda noqonuniy mayning faoliyati ham keng tarqalmoqda. Bu turdagi faoliyatda maynerlar belgilangan tartibni buzgan holda elektr quvvatidan noqonuniy

ISSN 3030-3907

foydalanishmoqda. Bunday jarayonlar energiya sarfini oshiradi va elektr tarmoqlarida turli muammolarni keltirib chiqaradi.

An'anaviy elektr sarfi bo'yicha monitoring tizimlari bunday yashirin jarayonlarni har doim ham aniqlay olmaydi. Shu sababli mashinani o'qitish usullaridan foydalangan holda tarmoq trafigi va tizim xatti-harakatlarini tahlil qilish noqonuniy mayning faoliyatini aniqlashda samarali yo'l sifatida qaralmoqda. Mashinani o'qitish usullari katta hajmdagi tizim ma'lumotlarini avtomatik tahlil qilib, anomal holatlarni aniqlashga imkon beradi. Bunday yondashuv tarmoq trafigi, jarayonlar faolligi yoki resurs sarfi kabi belgilar asosida noqonuniy mayning faoliyatini erta aniqlash imkonini beradi.

Tadqiqotning maqsadi — mashinani o'qitish usullaridan foydalangan holda mayning faoliyatini aniqlovchi model va algoritmni ishlab chiqish hamda uni amaliy sinovdan o'tkazishdir.

Tadqiqotning asosiy vazifalari:

1. Noqonuniy mayning faoliyatining texnik belgilarini aniqlash.
2. Ma'lumotlar to'plamini shakllantirish va xususiyatlar tanlash.
3. Mashinani o'qitish algoritmlarini sinovdan o'tkazish va samaradorlikni taqqoslash.
4. Olingan natijalar asosida optimal modelni taklif etish.

ADABIYOTLAR TAHLILI. Mashinani o'qitish usullari yordamida mayning faoliyatini aniqlash bo'yicha bir nechta tadqiqot ishlari amalga oshirilgan. A.Pastor va boshqalar faqat passiv tarmoq monitoringi orqali kiberjinoyatchilar tomonidan foydalanuvchi qurilmalariga o'rnatilgan zararli mayning dasturlarini aniqlash uchun yechim taklif etishgan [1]. Ular real vaqt rejimida mayning faoliyatidagi tarmoq oqimini aniqlash uchun mashinani o'qitish va chuqur o'qitish modellarining keng to'plami bilan birgalikda qo'llaniladigan yuqori ahamiyatli tarmoq oqimi xususiyatlarining yangi to'plamini ishlab chiqishdi. Yuqori informativ xususiyatlarning murakkab mashinani o'qitish modellari bilan kombinatsiyasidan foydalangan holda, hatto trafik shifrlangan bo'lsa ham, lokal tarmoqda mayning hujumlarini telekommunikatsiya darajasidagi aniqlik va to'g'rilik bilan aniqlash mumkinligini ko'rsatish uchun to'liq tajribalar majmuasi o'tkazildi.

M.A.M.Ariffin, R.R.Karn va boshqalar mayning faoliyatini bulutli hisoblash platformasida zararli dasturlar orqali amalga oshirilishi o'rgangan [2, 3]. Keraksiz mayning faoliyati doimiy protsessor ishlatish, sovitish ehtiyojlarini oshirish va foyda olinmagan hisoblashlar tufayli tashkilotga moliyaviy yo'qotishlarga olib keladi. Usulda bulutning tizim ko'rsatkichlari to'plangan, oldindan qayta ishlangan va keyin xususiyatlarni ajratib olish amalga oshirilgan. So'ngra, mayning faoliyati natijasida yuzaga keladigan shovqinni ajratish xususiyatlarining qiymatlarini qayta

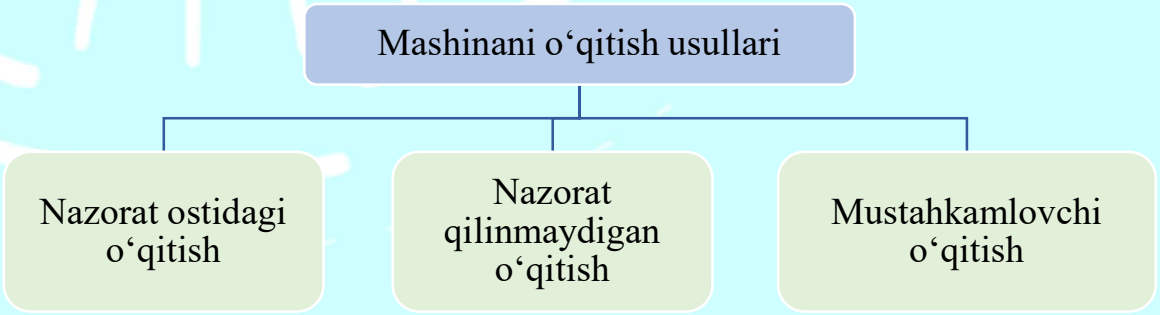
ISSN 3030-3907

ishlash uchun AD3 (Alternating Directions Dual Composition) algoritmi qo‘llanilgan. Taklif etilayotgan usulning samaradorligini baholash uchun OpenStack dasturida ishlaydigan bulutli platformada sinovdan o‘tkazildi va natija shuni ko‘rsatadiki, taklif etilayotgan usul mayning faoliyatini samarali aniqlash va uni boshqa fon faolligi shovqinlaridan farqlash imkonini beradi. Mayning faoliyati modellashtirilganda, belgilar zichligi qiymatlarining grafigi anomaliyani ko‘rsatadigan sezilarli pasayishni ko‘rsatadi.

TADQIQOT METODOLOGIYASI.

1. Mashinani o‘qitishning nazariy asoslari. Mashinani o‘qitish sun’iy intellektning bo‘limi bo‘lib, dasturiy ta’minotlarni dasturlashtirmagan holda natijalarni bashorat qilishni aniqroq bo‘lishiga imkon beradi. Ya’ni inson tabiatiga xos yaqin qarorlarni qabul qilishda qo‘llanilmoqda. Mashinani o‘qitish shunday sohaki, bunda kompyuterlar to‘g‘ridan-to‘g‘ri dasturlanmasdan o‘rganish qobiliyatiga ega bo‘ladi. Tasniflash, klasterlash, regressiya va chuqur o‘rganish mashinani o‘qitishdagi ba’zi modellardir. Ma’lumotlarning qay tarzda foydalanilishiga nisbatan mashinani o‘qitish usullarini uch turga bo‘lish mumkin (1-rasm) [4]:

- nazorat ostidagi o‘qitish;
- nazorat qilinmaydigan o‘qitish;
- mustahkamlovchi o‘qitish.



1-rasm. Mashinani o‘qitish usullari

Nazorat ostidagi o‘qitish algoritmlari keng tarqalgan usul bo‘lib, mashinani o‘qitish tizimiga oldindan aniqlangan ma’lumotlar taqdim etiladi va shu asosda u natijani bashorat qiladi. Spamni filtrlash nazoratli o‘qitishga misoldir.

Nazorat qilinmaydigan o‘qitish - bu mashina hech qanday nazoratsiz o‘rganadigan o‘qitish usulidir. O‘qitishda mashina tasniflanmagan yoki toifalanmagan ma’lumotlar to‘plami bilan ta’minlanadi va algoritm ushbu ma’lumotlarga hech qanday nazoratsiz harakat qilishi kerak bo‘ladi. Nazoratsiz o‘qitishning maqsadi kirish ma’lumotlarini yangi xususiyatlar yoki o‘xshashlik alomatlariga ega bo‘lgan obyektlar guruhiga ajratishdir.

Mustahkamlovchi o‘qitish - bu fikr-mulohazalarga asoslangan o‘rganish usuli bo‘lib, unda o‘quv aqlli agentdan (o‘zi mavjud bo‘lgan muhitda tajriba,

ISSN 3030-3907

foydalanuvchi kiritgan ma’lumotlar va turli shartlar asosida qaror qabul qila oladigan kompyuter dasturi elementi) har bir to‘g‘ri harakat uchun mukofot oladi va har bir noto‘g‘ri harakat uchun jazo oladi. Agent ushbu fikr-mulohazalar bilan avtomatik ravishda o‘rganadi va ish faoliyatini yaxshilaydi. Mustahkamlovchi o‘qitishda agent atrof-muhit bilan o‘zaro ta’sir qiladi va uni o‘rganadi. Jarayon davomida mukofot va jarima sifatida ball sistemasidan foydalaniladi. Ya’ni maqbul harakatlar bajarilganda ball beriladi va nomaqbul harakatlar uchun ball olib tashlanadi. Shu tariqa agent faqat maqbul harakatlarni bajarishga rag‘batlantiriladi. Mustahkamlovchi o‘qitishni haydovchisiz avtomobillar va biznesning marketing xarajatlarini optimallashtirishda foydalanish mumkin.

2. Mayning faoliyatining texnik belgilarini tahlil qilish. Noqonuniy mayning faoliyatini odatda quyidagi texnik belgilar orqali aniqlanishi mumkin [5]:

- CPU yoki GPU yuklanishining keskin ortishi;
- tarmoq trafigining o‘zgarishi;
- noma’lum domenlarga DNS so‘rovlar;
- tizimda yashirin jarayonlarning paydo bo‘lishi;
- elektr energiya sarfining ortishi.

Mazkur belgilar mashinani o‘qitish modellarini o‘qitishda xususiyatlar (features) sifatida qo‘llanilishi mumkin.

3. Taklif etilayotgan model konsepsiyasi. Tadqiqot doirasida mashinani o‘qitish usullari asosida mayning faoliyatini aniqlash uchun quyidagi konseptual bosqichlar taklif etiladi:

1. Ma’lumotlarni yig‘ish: tizim resurslari, jarayonlar, tarmoq oqimi haqidagi log fayllar.

2. Ma’lumotlarni qayta ishlash: tozalash, normalizatsiya, xususiyat tanlash.

3. Modelni o‘qitish: klassifikatsiya (Tasodifiy o‘rmon, Tayanch vektorlar usuli, Chuqur neyrotarmoq).

4. Natijalarni baholash: aniqlik, xato ehtimoli, yolg‘on pozitsiya va eslab qolish ko‘rsatkichlari asosida.

5. Real vaqt monitoring tizimiga integratsiya qilish.

MUHOKAMA VA NATIJALAR. Ushbu tadqiqotda amaliy ma’lumotlar asosida model sinovi o‘tkazilmagan bo‘lsa-da, konseptual tahlil natijasida quyidagi ilmiy xulosalarga kelindi:

- Mashinani o‘qitish usullari yordamida mayning faoliyatining turli texnik belgilarini birlashtirib, integrallashgan aniqlash tizimi yaratish mumkin.
- Mashinani o‘qitish modellar real vaqt rejimida o‘zini moslashtiruvchi monitoring tizimlari uchun mosdir.

ISSN 3030-3907

• Noqonuniy mayning faoliyatini aniqlashda xususiyatlar kombinatsiyasi muhim: faqat CPU yuklanishiga emas, balki tarmoq, energiya sarfi va jarayon tuzilmasiga asoslanish kerak.

Mashinani o‘qitish asosidagi yondashuvlar kiberxavfsizlik sohasida yangi bosqichni boshlab berdi.

Mayning faoliyatini aniqlashda bunday yondashuvlar quyidagi ustunliklarni beradi:

•*Moslashuvchanlik:* yangi turdagi mayning dasturlariga model qayta o‘qitishsiz moslasha oladi;

•*Avtomatlashtirish:* inson aralashuvisiz anomal holatlarni aniqlash imkonini beradi;

•*Aniqlik:* murakkab bog‘liklarni o‘rganish orqali xatolikni kamaytiradi.

Shu bilan birga, mashinani o‘qitish asosidagi tizimlarni joriy etishda ayrim cheklovlar mavjud:

•Katta hajmdagi o‘quv ma’lumotlari zarur;

•Modelning ishlashi kompyuter resurslariga bog‘liq;

•Yolg‘on pozitsiya ogohlantirishlarni kamaytirish uchun sinov bosqichlari muhim.

XULOSA VA TAKLIFLAR. Tadqiqot natijalari shuni ko‘rsatadiki, mashinani o‘qitish usullari mayning faoliyatini aniqlashda katta imkoniyatlarga ega.

Bu yondashuv yordamida:

•tizimdagi resurs sarfi va anomal jarayonlarni aniqlash;

•yangi turdagi yashirin mayning dasturlarini erta bosqichda fosh etish;

•tarmoq xavfsizligini oshirish mumkin.

Taklif etilgan nazariy model keyingi bosqichda amaliy tajribalar bilan boyitilib, kiberxavfsizlik sohasida avtomatlashtirilgan aniqlash tizimlari uchun asos bo‘la oladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Pastor A., Mozo A., Vakaruk S., Canavese D., Lopez D.R., Regano L., Gomes-Canaval S. and Lioy A. Detection of Encrypted Cryptomining Malware Connections With Machine and Deep Learning. Digital Object Identifier 10.1109/ACCESS. 2020. 3019658

2. Ariffin M.A.M., Darus M.Y., Taib A.M., Osman R., Mat Ch.M.A.Ch. Detecting Illicit Cryptocurrency Mining Activity in Cloud Computing Platform. Journal of Positive School Psychology. 2022, Vol. 6, No. 3, 8611–8622.

3. Karn R.R., Kudva P., Huang H., Suneja S. and Elfadel I.M. Cryptomining Detection in Container Clouds Using System Calls and Explainable Machine Learning. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 32, NO. 3, MARCH 2021.

ISSN 3030-3907

4. Kamalov S., Raxmatov Sh. Sun'iy intellekt asoslari. Mashinaviy o'qitish. T:. "Ijod NASHR" nashriyoti, 2022. – 104 b.
5. Nagar J. and Salai G. Machine Learning Based Cryptomining detection. Chennai 600 119.

ISSN 3030-3907