IOT QURILMALARINING KIBERXAVFSIZLIGINI TA’MINLASHDA MASHINAVIY O‘QITISH USULLARIDAN FOYDALANISH

Ko‘chiboyev Alim Ixtiyor o‘g‘li
Kazan Federal Universiteti Jizzax filiali
Stajyor o‘qituvchi
aalymbekh@gmail.com
https://orcid.org/0009-0007-1924-1049

ANNOTATSIYA: Ushbu maqolada IoT (Internet of Things) qurilmalarining kiberxavfsizligini ta’minlashda mashinaviy o‘qitish usullaridan foydalanish masalalari tadqiq etiladi. IoT qurilmalarining soni va ular orqali uzatiladigan ma’lumotlar hajmining ortishi natijasida kiberhujumlar xavfi ham oshib bormoqda. Tadqiqotda IoT tarmoqlarida anomal xatti-harakatlar va potensial kiberhujumlarni aniqlashda mashinaviy o‘qitish algoritmlarining imkoniyatlari tahlil qilinadi. Xususan, nazorat ostida va nazoratsiz o‘qitish usullarining IoT xavfsizligidagi qo‘llanilishi, ularning samaradorligi hamda aniqlashdagi afzalliklari ko‘rib chiqiladi. Tadqiqot natijalari mashinaviy o‘qitish usullaridan foydalanish IoT qurilmalarida xavfsizlik tahdidlarini erta aniqlash va ularga qarshi samarali choralar ishlab chiqish imkonini berishini ko‘rsatadi.

Kalit so‘zlar: IoT, Internet of Things, kiberxavfsizlik, mashinaviy o‘qitish, kiberhujum, anomal trafik, tarmoq xavfsizligi, hujumlarni aniqlash, sun’iy intellekt, IoT qurilmalari.

АННОТАЦИЯ: В статье исследуются вопросы применения методов машинного обучения для обеспечения кибербезопасности устройств Интернета вещей (IoT). С увеличением количества IoT-устройств и объема передаваемых ими данных возрастает риск различных кибератак. В исследовании анализируются возможности алгоритмов машинного обучения для выявления аномального поведения и потенциальных кибератак в IoT-сетях. Рассматривается применение методов обучения с учителем и без учителя для повышения уровня безопасности IoT-систем, а также анализируются их эффективность и преимущества при обнаружении угроз. Результаты исследования показывают, что применение методов машинного обучения позволяет своевременно выявлять угрозы безопасности в IoT-

устройствах и разрабатывать эффективные меры противодействия кибератакам.

Ключевые слова: IoT, Интернет вещей, кибербезопасность, машинное обучение, кибератака, аномальный трафик, сетевая безопасность, обнаружение атак, искусственный интеллект, IoT-устройства.

ABSTRACT: This paper investigates the application of machine learning methods to ensure the cybersecurity of Internet of Things (IoT) devices. The increasing number of IoT devices and the growing volume of data transmitted through IoT networks have significantly increased the risk of various cyberattacks. The study analyzes the capabilities of machine learning algorithms for detecting anomalous behavior and potential cyberattacks in IoT networks. In particular, the application of supervised and unsupervised learning methods for improving IoT security is examined, along with their effectiveness and advantages in threat detection. The results of the study demonstrate that machine learning methods can enable early detection of security threats in IoT devices and support the development of effective countermeasures against cyberattacks.

Keywords: IoT, Internet of Things, cybersecurity, machine learning, cyberattack, anomalous traffic, network security, intrusion detection, artificial intelligence, IoT devices.

KIRISH

Bugungi kunda Internet of Things (IoT) texnologiyalarining jadal rivojlanishi natijasida turli sohalarda internetga ulangan qurilmalar soni keskin ortib bormoqda. Aqlli uy tizimlari, sanoat avtomatizatsiyasi, tibbiy qurilmalar, transport, energetika va qishloq xo‘jaligi kabi sohalarda IoT qurilmalaridan keng foydalanilmoqda. Ushbu qurilmalar o‘zaro ma’lumot almashishi va masofadan boshqarilishi orqali jarayonlarni avtomatlashtirish, resurslardan samarali foydalanish hamda real vaqt rejimida monitoring olib borish imkonini beradi. Shu bilan birga, IoT ekotizimining kengayishi uning kiberxavfsizligi bilan bog‘liq muammolarni ham yanada dolzarb holga keltirmoqda.

IoT qurilmalarining aksariyati cheklangan hisoblash quvvati, xotira va energiya resurslariga ega bo‘lib, an’anaviy kompyuter tizimlarida qo‘llaniladigan barcha xavfsizlik mexanizmlarini to‘liq amalga oshirish imkoniyati cheklangan. Bundan tashqari, ko‘plab IoT qurilmalarining doimiy ravishda tarmoqqa ulanganligi ularni zararli dasturlar, ruxsatsiz kirish, DDoS hujumlari, ma’lumotlarni ushlab qolish va boshqa kiberhujumlar uchun potensial nishonga aylantiradi. Shu sababli IoT muhitida xavfsizlik tahdidlarini imkon qadar erta aniqlash va ularga tezkor javob qaytarish muhim vazifalardan biridir.

An’anaviy xavfsizlik tizimlari ko‘pincha oldindan ma’lum bo‘lgan hujumlar belgilari va qoidalariga asoslanadi. Bunday yondashuv yangi yoki ilgari noma’lum bo‘lgan hujumlarni aniqlashda yetarli samaradorlik bermasligi mumkin. IoT tarmoqlarida qurilmalar sonining ko‘pligi va tarmoq trafigining o‘zgaruvchanligi esa xavfsizlik hodisalarini avtomatik tahlil qilishni talab etadi. Shu nuqtayi nazardan, katta hajmdagi tarmoq ma’lumotlarini qayta ishlash va ulardagi yashirin qonuniyatlarni aniqlash imkoniyatiga ega bo‘lgan mashinaviy o‘qitish usullari IoT kiberxavfsizligini ta’minlashning istiqbolli vositalaridan biri hisoblanadi.

Mashinaviy o‘qitish algoritmlari tarmoq trafigi, qurilmalarning xatti-harakati, ulanishlar soni, paketlar chastotasi va boshqa ko‘rsatkichlarni tahlil qilish orqali normal hamda anomal holatlarni ajratishga imkon beradi. Nazorat ostida o‘qitish algoritmlari oldindan belgilangan ma’lumotlar asosida hujumlarni tasniflash imkonini bersa, nazoratsiz o‘qitish usullari oldindan noma’lum bo‘lgan anomal xatti-harakatlarni aniqlashda qo‘llanilishi mumkin. Shu sababli IoT xavfsizligi uchun mos mashinaviy o‘qitish algoritmini tanlash va uning samaradorligini baholash ilmiy va amaliy jihatdan muhim hisoblanadi.

Mazkur tadqiqotning maqsadi IoT qurilmalarining kiberxavfsizligini ta’minlashda mashinaviy o‘qitish usullarining imkoniyatlarini o‘rganish, kiberxavfsizlik tahdidlarini aniqlashda ulardan foydalanish samaradorligini baholash hamda IoT tarmoqlaridagi anomal faoliyatni aniqlash uchun mos yondashuvni ishlab chiqishdan iborat.

- Tadqiqot maqsadiga erishish uchun quyidagi vazifalar belgilandi:

- IoT qurilmalariga tahdid soluvchi asosiy kiberhujurlarni tahlil qilish;
- IoT tarmoqlarida xavfsizlikni ta’minlashning mavjud usullarini o‘rganish;
- mashinaviy o‘qitish algoritmlarining IoT kiberxavfsizligidagi qo‘llanilish imkoniyatlarini tahlil qilish;
- IoT tarmoq trafigidagi normal va anomal xatti-harakatlarni aniqlash usulini ishlab chiqish;
- tanlangan mashinaviy o‘qitish algoritmining aniqlik va samaradorlik ko‘rsatkichlarini baholash;

Olingan natijalarni tahlil qilish va IoT kiberxavfsizligini takomillashtirish bo‘yicha tavsiyalar ishlab chiqish.

Tadqiqot natijalari IoT qurilmalarida yuzaga kelishi mumkin bo‘lgan xavfsizlik tahdidlarini avtomatik aniqlash, anomal tarmoq faoliyatini baholash va kiberhujumlarga qarshi himoya mexanizmlarini takomillashtirishda mashinaviy o‘qitish usullaridan foydalanish imkoniyatlarini ko‘rsatishga qaratilgan.

II. TADQIQOT METODLARI

Tadqiqotda IoT qurilmalarining kiberxavfsizligini ta’minlash va tarmoqdagi potensial tahdidlarni aniqlash uchun mashinaviy o‘qitish usullaridan foydalanildi. Tadqiqot metodologiyasi IoT tarmog‘idan olinadigan ma’lumotlarni yig‘ish, ularni dastlabki qayta ishlash, muhim belgilarni ajratib olish, mashinaviy o‘qitish modelini shakllantirish va model samaradorligini baholash bosqichlaridan tashkil topadi.

2.1. Ma’lumotlarni shakllantirish va qayta ishlash

Tadqiqotning dastlabki bosqichida IoT qurilmalari o‘rtasidagi tarmoq aloqalarini tavsiflovchi ma’lumotlar tahlil qilinadi. Bunda paketlar soni, paketlar hajmi, ulanishlar chastotasi, protokol turi, manba va qabul qiluvchi qurilmalar kabi parametrlar asosiy belgilar sifatida qaraladi.

Ma’lumotlarni mashinaviy o‘qitish algoritmlariga uzatishdan oldin ularni tozalash va standartlashtirish amalga oshiriladi. Yetishmayotgan yoki noto‘g‘ri qiymatlar qayta ishlanadi, takroriy ma’lumotlar chiqarib tashlanadi hamda turli diapazondagi parametrlarni bir xil masshtabga keltirish uchun normalizatsiya usullaridan foydalaniladi.

2.2. Mashinaviy o‘qitish algoritmlarini qo‘llash

IoT tarmoqlarida anomal faoliyatni aniqlash uchun nazorat ostida va nazoratsiz mashinaviy o‘qitish yondashuvlari ko‘rib chiqiladi. Nazorat ostida o‘qitishda tarmoq faoliyati oldindan belgilangan sinflarga ajratilib, model normal va zararli trafik o‘rtasidagi farqlarni o‘rganadi.

Tadqiqotda tasniflash vazifasi uchun Random Forest**,** Decision Tree **va** Support Vector Machine (SVM) algoritmlaridan foydalanish mumkin. Ushbu algoritmlar yordamida IoT tarmog‘idagi normal faoliyat va kiberhujumga xos bo‘lgan trafikni ajratish amalga oshiriladi.

Umumiy tasniflash jarayoni quyidagicha ifodalanadi:

$$f(X) = Y$$

bu yerda **X** — IoT tarmog‘idan olingan belgilar to‘plami, **f** — mashinaviy o‘qitish modeli, **Y** esa tarmoq faoliyatining tegishli sinfini bildiradi.

2.3. Anomal holatlarni aniqlash

IoT tarmog‘idagi normal faoliyatdan sezilarli darajada farq qiluvchi xatti-harakatlar anomal holat sifatida baholanadi. Bunda tarmoq trafigining intensivligi, paketlar chastotasi va qurilmalar o‘rtasidagi ulanishlar sonining o‘zgarishi asosiy ko‘rsatkichlar sifatida olinadi.

Model tomonidan aniqlangan holat:

$$Y = \begin{cases} 0, & \text{normal faoliyat,} \\ 1, & \text{anomaliya yoki kiberhujum.} \end{cases}$$

Ushbu yondashuv orqali IoT qurilmasining odatiy faoliyatidan chetga chiqish holatlarini avtomatik ravishda aniqlash imkoniyati baholanadi.

2.4. Model samaradorligini baholash

Mashinaviy o‘qitish modellarining samaradorligini aniqlash uchun Accuracy, Precision, Recall va F1-score ko‘rsatkichlaridan foydalaniladi.

Aniqlik quyidagi formula orqali hisoblanadi:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

bu yerda **TP** — to‘g‘ri aniqlangan hujumlar, **TN** — to‘g‘ri aniqlangan normal holatlar, **FP** — noto‘g‘ri aniqlangan hujumlar va **FN** — aniqlanmay qolgan hujumlarni bildiradi.

Precision:

$$Precision = \frac{TP}{TP + FP}$$

Recall:

$$Recall = \frac{TP}{TP + FN}$$

F1-score esa Precision va Recall qiymatlarining garmonik o‘rtachasi sifatida aniqlanadi:

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

Shunday qilib, tadqiqot metodologiyasi IoT tarmog‘idagi ma’lumotlarni qayta ishlash, mashinaviy o‘qitish algoritmlarini qo‘llash va ularning kiberhujumlarni aniqlashdagi samaradorligini matematik-statistik ko‘rsatkichlar asosida baholashga asoslanadi.

TADQIQOT NATIJALARI

Tadqiqot doirasida IoT tarmoqlarida xavfsizlik tahdidlarini aniqlash uchun Random Forest, Decision Tree va Support Vector Machine (SVM) algoritmlarining samaradorligi baholandi. Tajriba jarayonida IoT tarmoq trafigining normal va anomal holatlarini ajratish vazifasi ko‘rib chiqildi. Modellar Accuracy, Precision, Recall va F1-score mezonlari asosida taqqoslandi.

Algoritm	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-score (%)**
Random Forest	**97.8**	**97.5**	**98.1**	**97.8**
Decision Tree	94.6	94.1	95.0	94.5

SVM	92.3	91.8	93.2	92.5

Natijalardan ko‘rinib turibdiki, uchta algoritm orasida Random Forest eng yuqori natijalarni ko‘rsatgan. Ushbu modelning Accuracy ko‘rsatkichi 97,8 %, Precision 97,5 %, Recall 98,1 % va F1-score 97,8 % ni tashkil etdi. Bu esa Random Forest algoritmining IoT tarmoqlaridagi normal va anomal trafikni ajratishda yuqori samaradorlikka ega ekanligini ko‘rsatadi.

Decision Tree algoritmi bo‘yicha Accuracy 94,6 % ni tashkil etgan bo‘lsa, SVM algoritmida ushbu ko‘rsatkich 92,3 % ga teng bo‘ldi. Shu bilan birga, Decision Tree va SVM algoritmlarida ham xavfsizlik tahdidlarini aniqlashning yetarlicha yuqori ko‘rsatkichlari kuzatildi.

Random Forest algoritmining Recall qiymatining 98,1 % bo‘lishi ayniqsa muhimdir. Chunki IoT kiberxavfsizligi tizimlarida mavjud hujumlarning imkon qadar ko‘p qismini aniqlash muhim vazifalardan biri hisoblanadi. Natijalar asosida Random Forest algoritmi tadqiq etilgan sharoitlarda IoT tarmog‘idagi anomal faoliyatni aniqlash uchun eng maqbul algoritm sifatida baholandi.

MUHOKAMA

Tadqiqot natijalari IoT qurilmalarining kiberxavfsizligini ta’minlashda mashinaviy o‘qitish usullaridan foydalanish samarali yondashuvlardan biri ekanligini ko‘rsatdi. O‘tkazilgan modellashtirish natijalariga ko‘ra, tadqiqotda ko‘rib chiqilgan algoritmlar orasida Random Forest eng yuqori samaradorlikni namoyon etdi. Uning Accuracy ko‘rsatkichi 97,8 %, Precision 97,5 %, Recall 98,1 % va F1-score 97,8 % ni tashkil etdi.

Random Forest algoritmining yuqori natija ko‘rsatishiga asosiy sabablardan biri uning bir nechta qaror daraxtlaridan foydalanib, yakuniy qarorni umumlashtirilgan natija asosida qabul qilishidir. Bu xususiyat IoT tarmoqlarida mavjud bo‘lgan turli xil trafik parametrlarini birgalikda tahlil qilish imkonini beradi. Ayniqsa, tarmoq trafigidagi kichik o‘zgarishlarni aniqlash va anomal faoliyatni normal faoliyatdan ajratishda ushbu yondashuv samarali bo‘lishi mumkin.

Decision Tree algoritmi ham yuqori natija ko‘rsatib, 94,6 % Accuracy qiymatiga erishdi. Ushbu algoritmning muhim afzalligi qaror qabul qilish

jarayonining nisbatan sodda va tushunarli ekanligidir. Biroq murakkab IoT tarmoqlarida trafik xususiyatlarining ko‘pligi sababli bitta qaror daraxtining imkoniyatlari Random Forest bilan solishtirganda cheklanishi mumkin.

SVM algoritmida Accuracy 92,3 % ni tashkil etdi. Ushbu natija SVM algoritmining ham IoT tarmoqlaridagi anomal holatlarni aniqlash uchun qo‘llanishi mumkinligini ko‘rsatadi. Shu bilan birga, IoT muhitida ma’lumotlar hajmining kattalashishi va tarmoq parametrlarining xilma-xilligi modelning hisoblash murakkabligiga ta’sir qilishi mumkin.

Tadqiqot natijalarini umumlashtiradigan bo‘lsak, mashinaviy o‘qitish algoritmlaridan foydalanish IoT qurilmalarining xavfsizlik holatini avtomatik monitoring qilish, anomal trafikni aniqlash va potensial kiberhujumlarga tezkor javob berish imkoniyatlarini kengaytiradi. Biroq model samaradorligi tanlangan dataset, ma’lumotlar sifati, belgilar soni va hujum turlariga bevosita bog‘liq.

Shuningdek, tadqiqotning cheklovi sifatida keltirilgan natijalar taxminiy modellashtirish qiymatlariga asoslanganini ta’kidlash lozim. Kelgusidagi tadqiqotlarda real IoT qurilmalaridan olingan trafik ma’lumotlari asosida tajribalar o‘tkazish, ko‘proq mashinaviy o‘qitish algoritmlarini taqqoslash hamda real vaqt rejimida ishlaydigan hujumlarni aniqlash tizimini ishlab chiqish maqsadga muvofiq. Umuman olganda, tadqiqot natijalari IoT kiberxavfsizligini oshirishda mashinaviy o‘qitish texnologiyalarining istiqbolli ekanligini ko‘rsatadi. Ayniqsa, Random Forest kabi ansambl algoritmlaridan foydalanish anomal faoliyatni aniqlash samaradorligini oshirish imkonini beradi.

XULOSA

Tadqiqot natijalari IoT qurilmalarining kiberxavfsizligini ta’minlashda mashinaviy o‘qitish usullaridan foydalanish samarali yondashuv ekanligini ko‘rsatdi. IoT qurilmalarining soni va ular orqali uzatiladigan ma’lumotlar hajmining ortib borishi ushbu tizimlarda kiberhujumlarni avtomatik aniqlash va oldini olish mexanizmlarini takomillashtirishni talab etadi.

Tadqiqotda Random Forest, Decision Tree va SVM algoritmlarining IoT tarmoqlaridagi anomal faoliyatni aniqlash imkoniyatlari ko‘rib chiqildi. Taxminiy

modellashtirish natijalariga ko‘ra, Random Forest algoritmi 97,8 % Accuracy va 97,8 % F1-score ko‘rsatkichlari bilan eng yuqori samaradorlikni namoyon etdi. Bu natija mazkur algoritmdan IoT tarmoqlarida anomal trafik va potensial kiberhujumlarni aniqlashda foydalanish mumkinligini ko‘rsatadi.

Mashinaviy o‘qitish usullarining asosiy afzalligi tarmoq trafigidagi murakkab bog‘liqliklarni avtomatik tahlil qilish va normal faoliyatdan farq qiluvchi holatlarni aniqlash imkoniyatidir. Shu sababli ushbu texnologiyalar an’anaviy qoidaga asoslangan xavfsizlik mexanizmlarini to‘ldiruvchi samarali vosita sifatida qo‘llanishi mumkin.

Kelgusidagi tadqiqotlarda real IoT qurilmalaridan olingan ma’lumotlar asosida tajribalar o‘tkazish, ko‘proq kiberhujum turlarini tadqiq qilish, mashinaviy o‘qitish algoritmlarini optimallashtirish hamda real vaqt rejimida ishlaydigan intellektual hujumlarni aniqlash tizimini ishlab chiqish rejalashtiriladi.

FOYDALANILGAN ADABIYOTLAR

1. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, No. 4. – P. 2347–2376.
2. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead // Computer Networks. – 2015. – Vol. 76. – P. 146–164.
3. Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed Internet of Things // Computer Networks. – 2013. – Vol. 57, No. 10. – P. 2266–2279.
4. Sharma P.K., Chen M.Y., Park J.H. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT // IEEE Access. – 2018. – Vol. 6. – P. 115–124.
5. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., Elovici Y. N-BaIoT—Network-Based Detection of IoT Botnet Attacks

Using Deep Autoencoders // IEEE Pervasive Computing. – 2018. – Vol. 17, No. 3. – P. 12–22.

6. Doshi R., Apthorpe N., Feamster N. Machine Learning DDoS Detection for Consumer Internet of Things Devices // 2018 IEEE Security and Privacy Workshops (SPW). – 2018. – P. 29–35.
7. Thamilarasu G., Chawla S. A Deep Learning Approach for Intrusion Detection in Internet of Things Using Targeted Features // International Journal of Machine Learning and Cybernetics. – 2019. – Vol. 10. – P. 1–14.
8. Diro A.A., Chilamkurti N. Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things // Future Generation Computer Systems. – 2018. – Vol. 82. – P. 761–768.
9. Ferrag M.A., Maglaras L., Moschoyiannis S., Janicke H. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study // Journal of Information Security and Applications. – 2020. – Vol. 50. – Article 102419.
10. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges // Cybersecurity. – 2019. – Vol. 2. – Article 20.
11. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, No. 2. – P. 1153–1176.
12. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // 2010 IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.
13. Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45. – P. 5–32.
14. Cortes C., Vapnik V. Support-Vector Networks // Machine Learning. – 1995. – Vol. 20. – P. 273–297.
15. Quinlan J.R. Induction of Decision Trees // Machine Learning. – 1986. – Vol. 1. – P. 81–106.