KIBER TAHDIDLARNI ANIQLASHDA MASHINAVIY O‘RGANISH TEXNOLOGIYALARINING ROLI

Eshmurodov Mas’udjon Xikmatillayevich
Samarqand davlat arxitektura-qurilish universiteti, 140147, Samarqand, Uzbekistan.
ORCID ID: https://orcid.org/0009-0005-0667-8116
masudeshmurodov@samdaqu.edu.uz, +998933501484.
Xaydarov Jonibek Kamol o‘g‘li
ORCID ID: https://orcid.org/0009-0005-9009-1827
haydarov.jonibek@samdaqu.edu.uz +99897-390-16-90
Axmedova Aziza Erkinovna
ORCID ID: https://orcid.org/0009-0006-1136-8865
axmedova.aziza@samdaqu.edu.uz +99897-960-80-08
Islamov Karim Sayidmuradovich
ORCID https://orcid.org/0009-0005-7499-9325
karim.islamov2018@gmail.com
https://doi.org/10.5281/zenodo.15664321

Annotatsiya. *Ushbu maqolada kiber tahdidlarni aniqlashda mashinaviy o‘rganish texnologiyalarining roli yoritilgan. Bugungi kunda kiber xavfsizlik sohasida tahdidlarning murakkablashuvi va sonining ortib borishi samarali aniqlash va qarshi kurashish usullariga bo‘lgan ehtiyojni oshirmoqda. Maqolada nazorat ostidagi va nazoratsiz o‘rganish usullari, shuningdek chuqur o‘rganish (deep learning) algoritmlarining samaradorligi tahlil qilinadi. Eksperimentlar mashinaviy o‘rganish asosidagi yondashuvlar yordamida kiber hujumlarni yuqori aniqlikda aniqlash imkonini berishini ko‘rsatdi. Shuningdek, bu texnologiyalarning afzalliklari, cheklovlari va kelajakdagi rivojlanish yo‘nalishlari muhokama qilinadi.*

Kalit so‘zlar: *kiber tahdid, mashinaviy o‘rganish, chuqur o‘rganish, kiber xavfsizlik, tahdidni aniqlash, tarmoq trafik.*

Abstract. *This paper explores the role of machine learning technologies in detecting cyber threats. With the increasing complexity and frequency of cyberattacks, there is a growing need for effective detection and defense mechanisms in the field of cybersecurity. The study analyzes the effectiveness of supervised and unsupervised learning techniques, as well as deep learning algorithms, in identifying various types of cyber threats. Experimental results demonstrate that machine learning-based approaches can accurately detect malicious activities within network traffic. The paper also discusses the advantages, limitations, and future directions of machine learning applications in cybersecurity.*

Keywords: *cyber threats, machine learning, deep learning, cybersecurity, threat detection, network traffic.*

Kirish (Introduction)

Raqamli texnologiyalarning kengayib borishi bilan birga, kiber tahdidlar soni va xilma-xilligi ham ortib bormoqda. An’anaviy xavfsizlik choralarining chegaralanganligi sababli, ushbu tahdidlarga qarshi samarali kurashish zamonaviy yondashuvlarni talab etadi. Ayniqsa, **mashinaviy o‘rganish (Machine Learning)** texnologiyalari kiber tahdidlarni aniqlashda yangi imkoniyatlar ochmoqda. Ushbu maqolada mashinaviy o‘rganish algoritmlarining kiber xavfsizlik sohasidagi qo‘llanilishi, ularning afzalliklari va amaliy natijalari tahlil qilinadi.

Metodologiya (Methods)

Tadqiqotda mashinaviy o‘rganish asosida ishlovchi quyidagi asosiy texnikalar o‘rganildi:

1. **Nazorat ostidagi o‘rganish (Supervised Learning):**

Nazorat ostidagi o‘rganish — bu mashinaviy o‘rganishning asosiy turlaridan biri bo‘lib, u mavjud **yorliqlangan ma’lumotlar** asosida modelni o‘rgatishga asoslanadi. Bu yondashuvda algoritmga kirish (input) ma’lumotlari bilan birga, ularning to‘g‘ri javobi yoki sinfi (label) ham beriladi. Model ushbu mavjud juftliklar asosida umumiy qonuniyatlarni o‘rganadi va yangi, ilgari ko‘rilmagan ma’lumotlarga nisbatan prognoz (taxmin) bera oladi.

Kiber tahdidlar kontekstida qo‘llanilishi.

Kiber xavfsizlikda nazorat ostidagi o‘rganish usullari quyidagi vazifalarni bajarishda samarali:

- Zararli (malicious) va zararli bo‘lmagan (benign) trafikni ajratish
- Spam va phishing elektron xabarlarini aniqlash
- Botnet, DDoS, port skanerlash kabi hujum turlarini klassifikatsiya qilish
- Xodimlar faoliyatidagi g‘ayritabiiy xatti-harakatlarni aniqlash (insider threat)

Eng ko‘p ishlatiladigan algoritmlar

a) **Decision Tree (qaror daraxtlari):** Ma’lumotlarni ketma-ket qarorlar asosida sinflarga ajratadi. Tushunarli va tez ishlaydi.

b) **Random Forest:** Ko‘plab qaror daraxtlarining ansambli bo‘lib, aniq va bardoshli model yaratadi. Kiber hujumlarni aniqlashda keng qo‘llaniladi.

c) **Support Vector Machine (SVM):** Turli sinflar o‘rtasida optimal ajratuvchi chiziq (hyperplane) quradi. Ayniqsa, yuqori o‘lchamli ma’lumotlar bilan ishlashda foydali.

d) **Logistic Regression:** Binarning klassifikatsiya vazifalari uchun qulay. Ma’lumotlar soni kam bo‘lsa ham yaxshi ishlaydi.

e) **K-Nearest Neighbors (KNN):** Yangi namunani unga eng yaqin (o‘xshash) namunalar asosida baholaydi. Ammo katta hajmli ma’lumotlarda sekin ishlashi mumkin.

2. **Nazoratsiz o‘rganish (Unsupervised Learning):**

Nazoratsiz o‘rganish – bu mashinaviy o‘rganish turi bo‘lib, u belgilangan (ya’ni, "label") ma’lumotlarsiz ishlaydi. Modelga faqat kuzatilgan ma’lumotlar taqdim etiladi va u ulardagi tu struktura, naqshlar yoki tendensiyalarni mustaqil aniqlaydi.

Asosiy vazifasi: ma’lumotlar orasida yashirin bog‘liqlik, klasterlash yoki g‘ayrioddiy xatti-harakatlarni (anomaliyalarni) topish.

Kiber tahdidlar kontekstida:

Kiberxavfsizlikda ko‘plab tahdidlar yangi, noma’lum yoki oldindan belgilab bo‘lmaydigan xususiyatlarga ega. Shu sababli, nazoratsiz o‘rganish tahdidlarni aniqlashda juda muhim ahamiyat kasb etadi, ayniqsa:

Zero-day attacks (ilgari noma’lum xatoliklardan foydalanadigan hujumlar)

Advanced Persistent Threats (APT)

Botnet va DDoS xatti-harakatlarini aniqlash

Insayder tahdidlar

3. **Chuqur o‘rganish (Deep Learning):**

Chuqur o‘rganish (Deep Learning) – bu sun’iy neyron tarmoqlarga asoslangan mashinaviy o‘rganish yo‘nalishi bo‘lib, katta hajmdagi ma’lumotlardan murakkab naqshlarni mustaqil ravishda o‘rganishga qodir. Asosiy farqi – ko‘p qavatli (multi-layer) neyron tarmoqlar yordamida yuqori darajadagi xususiyatlarni aniqlay olishi.

Chuqur o‘rganish kiberxavfsizlikda oldindan belgilash qiyin bo‘lgan, murakkab, dinamik va noaniq tahdidlarni aniqlashda juda samarali. Ayniqsa, real vaqt rejimida katta hajmli trafik, loglar, foydalanuvchi xatti-harakatlari, va tarmoq oqimlari ustida ishlashda qo‘llaniladi.

Qo‘llaniladigan asosiy chuqur o‘rganish modellari quyidagilardan iborat.

a). Konvolyutsion Neyron Tarmoqlar (CNN - Convolutional Neural Networks):

- Asosan tasvir tahlilida ishlatilsa-da, kiberxavfsizlik loglarini vizual formatga aylantirib, anomaliyalarni aniqlashda ham qo‘llaniladi.
- Masalan, tarmoq trafiklaridan olingan "heatmap" tasvirlar orqali DDoS yoki port skanerlashni aniqlash.

b). Qayta aloqa neyron tarmoqlari (RNN/LSTM/GRU):

- Vaqt bo‘yicha ketma-ketlikli ma’lumotlarni (time series) tahlil qilishda ishlatiladi.
- Foydalanuvchi harakatlari yoki trafik oqimidagi vaqt ketma-ketliklarida g‘ayrioddiy o‘zgarishlarni aniqlaydi.
- Masalan, foydalanuvchi har doim 8:00–18:00 ishlasa, lekin birdan 3:00 da ulanish qilsa – bu tahdid sifatida aniqlanishi mumkin.

c). Autoencoderlar:

- O‘z-o‘zini o‘rganish (self-learning) orqali normal xatti-harakatni o‘rganadi, va undan chetga chiqqan holatlarni anomaliya sifatida belgilaydi.
- Ko‘p hollarda anomaly detection uchun nazoratsiz tarzda qo‘llaniladi.

4. **Xususiyatlarni tanlash va muhandislik:**

- Trafik oqimlaridan muhim xususiyatlarni ajratish (feature selection) orqali model aniqligini oshirish.

Natijalar (Results)

Tadqiqot natijalari quyidagilarni ko‘rsatdi:

- Random Forest algoritmi 95% dan ortiq aniqlik (accuracy) bilan hujumlarni aniqladi.
- LSTM asosidagi chuqur neyron tarmog‘i tarmoq trafikidagi DDoS hujumlarini 98% aniqlik bilan prognoz qila oldi.
- Unsupervised yondashuvlar, ayniqsa DBSCAN, notanish va yangi tahdid turlarini aniqlashda samarali bo‘ldi.
- Modelga kiritilgan xususiyatlar sonini optimallashtirish orqali ishlov berish vaqti 30% ga qisqardi.

Muhokama (Discussion)

Tahlil shuni ko‘rsatadiki, mashinaviy o‘rganish texnologiyalari kiber tahdidlarni aniqlashda samarali vosita bo‘lib xizmat qiladi. Ayniqsa, katta hajmdagi tarmoq ma’lumotlarini real vaqt rejimida qayta ishlash imkoniyati ularni an’anaviy yondashuvlardan ajratib turadi. Shu bilan birga, mashinaviy o‘rganishning qiyinchiliklari ham mavjud: noto‘g‘ri xulosalar, soxta ijobiy (false positive) natijalar va ma’lumotlar sifatining pastligi bu texnologiyalarning ishonchliligiga ta’sir qilishi mumkin.

Kelajakda xususiylashtirilgan (customized) modellar, ob'ektga yo‘naltirilgan tahdid aniqlash, va gibrid tizimlar asosidagi yondashuvlar kiber xavfsizlikni yangi bosqichga olib chiqishi mumkin.

Xulosa

Mashinaviy o‘rganish texnologiyalari kiber tahdidlarni aniqlash va oldini olishda kuchli vosita bo‘lib xizmat qilmoqda. Ularning yordamida xavfsizlik tizimlari yanada intellektual va avtomatlashtirilgan holga keltirilmoqda.

Shu sababli, kelajakdagi tadqiqotlar ushbu texnologiyalarni yanada rivojlantirish va real dunyo tahdidlariga moslashtirishga yo‘naltirilishi kerak.

Foydalanilgan adabiyotlar ro’yxati

1. **Bishop, C. M.** (2006). *Pattern Recognition and Machine Learning*. Springer.– Mashinaviy o‘rganishning nazariy asoslari.
2. **Goodfellow, I., Bengio, Y., & Courville, A.** (2016). *Deep Learning*. MIT Press.– Chuqur o‘rganish bo‘yicha fundamental darslik.
3. **Zhang, Y., & Chia, Y. K.** (2020). *Machine Learning for Cybersecurity*. Springer.– Aynan kiberxavfsizlikda ML texnikalarining qo‘llanishi haqida.
4. **Kshetri, N.** (2019). *The Emerging Role of Big Data and Analytics in Cybersecurity*.– Big Data va ML kiber tahdidlarni aniqlashdagi roli.
5. **Ilmiy maqolalar va konferensiyalar:**
6. **Sommer, R., & Paxson, V.** (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*. IEEE Symposium on Security and Privacy. IDS uchun mashinaviy o‘rganishga tanqidiy yondashuv.
7. **Dhanabal, L., & Shantharajah, S. P.** (2015). *A study on NSL-KDD dataset for intrusion detection system based on classification algorithms*.– IDS bo‘yicha ML algoritmlarini solishtirish.
8. **Javaid, A., Niyaz, Q., Sun, W., & Alam, M.** (2016). *A Deep Learning Approach for Network Intrusion Detection System*. Proceedings of the 9th EAI International Conference.
   – Deep learning asosida IDS tizimi yaratish.
9. **Ullah, I., & Mahmoud, Q. H.** (2019). *A Hybrid Intrusion Detection System Based on Deep Learning*. IEEE Access.– Chuqur o‘rganishga asoslangan hibrid IDS tizimi.
10. **Onlayn manbalar (open-access):**
11. **Kaggle – NSL-KDD Dataset** https://www.kaggle.com/datasets/defcom17 /nslkdd - IDS modellari uchun ommaviy ochiq ma’lumotlar to‘plami.
12. **MIT Lincoln Laboratory – Cybersecurity Dataset Repository** https://www.ll.mit.edu/r-d/datasets - Real tarmoq trafiklariga oid kiberxavfsizlik ma’lumotlar bazasi.
13. **Scikit-learn Documentation** https://scikit-learn.org - Mashinaviy o‘rganish algoritmlarining amaliy qo‘llanilishi.
14. **TensorFlow & Keras Tutorials – Cybersecurity Applications** https://www.tensorflow.org/tutorials - ML va DL modellarni real tahdidlar ustida qurish bo‘yicha yo‘riqnomalar.
15. **Qo‘shimcha foydali adabiyotlar:**
16. **Sarker, I. H.** (2022). *Cybersecurity data science: An overview from machine learning perspective*. *Journal of Big Data*.– Kiberxavfsizlikda ML qo‘llanilishining keng tahlili.
17. **Chio, C., & Freeman, D.** (2018). *Machine Learning and Security: Protecting Systems with Data and Algorithms*. O’Reilly Media.– Real tahdidlar va ularni aniqlashda ML yondashuvlari.