KOMPYUTER TARMOQLARIDA MAXFIY MA’LUMOTLARNI AI ASOSIDAGI ANIQLASH METODLARI

Alayev Ruhillo Habibovich[1], Nabiyev Xolbek Tolib o‘g‘li[1]

[1]“Mirzo Ulug‘bek” nomidagi O‘zbekiston Milliy Universiteti
E-mail: nabiyevxolbek2000@gmail.com

K E Y W O R D S

Kompyuter tarmoqlari,axborot xavfsizligi, AI(sun’iy intellekt),mashinaviy o‘rganish, anomaliyalarni aniqlash

A B S T R A C T

Mazkur maqolada, kompyuter tarmoqlarida uzatilayotgan va saqlanayotgan konfidentsial axborotlarni AI (Sun’iy intellekt) metodlari yordamida aniqlash yondashuvlari to‘g‘risida fikr yuritiladi.Hozirgi murakkab va dinamik tarmoq muhitida an’anviy yondashuvlar asosida tarmoqdagi ma’lumotlarni aniqlash yoki sizib chiqishini oldini olish yetarlicha foyda bermayotgani sababli mashinali o‘rganish va chuqur o‘rganish modellari tahlil qilinadi. Tadqiqotda klassifikatsiya va anomal holatlarni aniqlash usullarining ustunligi shuningdek ularni real tarmoq muhitida qo‘llashga doir fikr yuritiladi. Natijalar AI asosidagi metodlar kompyuter tarmoqlarida axborot xavfsizligini oshirishda muhim ahamiyatga ega ekanligini ko‘rsatadi.

Kalit so‘zlar:

Bugungi kunda yirik kompaniyalardan tortib kichik davlat idoralarida ham shuningdek moliya tizimlari, sog‘liqni saqlash , ta’lim sohalarida xodimlar va foydalanuvchilar o‘rtasida samarali va xavfsiz axborot almashinuvi jarayonini ta’minlash maqsadida kompyuter tarmoqlariga suyanadilar. Kompyuter tarmoqlari orqali turli xildagi konfidensial ma‘lumotlar almashinuvi va ularni qayta ishlash va saqlash mumkin va bu jarayonda xavfsizlikka tahdid soluvchi kiberhujumlar, ruxsatsiz kirishlar va ma’lumotlarni sizib chiqishi holatlari dolzarb muammolardan bir hisoblanadi.Bugungi kunda tarmoqdagi axborot almashinuv jarayoni va axborot hajmining keskin oshishi oqibatida tarmoqdagi ma’lumotlarni aniqlash,tasniflash va ularni monitoring qilish bilan bog‘liq muammolar yuzaga chiqdi. Kompyuter tarmoqlarida bir vaqtning o‘zida konfidentsial axborotlar ham oddiy ma’lumotlar orasida aralsh holatda uztiladi.

Maxfiy ma’lumotlar – bu sir saqlanadigan va o‘zgartirilishi yoki yo‘qotilishi salbiiy holatga yetaklaydigan axborotlardir, bunga misol qilib;

- Shaxsiy ma’lumotlar(pasport, biometrik ma’lumotlar va login parollar
- Moliyaviy ma’lumotlar(bank hisob raqamlari, tranzaksiyalar, kreditkarta m’lumotlari
- Korporativ ma’lumotlar(tijorat sirlari, bisnes ma’lumotlari va qimmatli qog‘ozlar)
- Davlat va maxsus ma’lumotlar v.h.k.

Tarmoq trafikida ushbu axborotlarni real vaqt rejimida aniqlash tarmoq xavfsizligini boshqarish, monitoring qilish va tahdidlarni baholash jarayonlarining asosiy qismi hisoblanadi. Muhim axborotni aniqlash jarayoni tarmoq paketlari tarkibi , uzatish kontekstini va ularning hatti harakatini tahlil qilishga asoslanadi.Muhim axborotlarni aniqlash tarmoqni himoyalashdan oldingi qadam sifatida belgilanadi, sababi shundaki agar tarmoqda qanday axborot uztilayotgani aniq ko‘rsatilmasa xatarni baholash va nazorat kabi navbatdagi bosqichlar smarali amalga oshmaydi.

Maxfiy ma’lumotlarni aniqlash –bu tarmoqda uzatilayotgan yoki saqlanayotgan ma’lumotlar ichidan muhim bo‘lgan ma’lumotlarni aniqlash va ajratib olish demakdir

Aniqlash jarayonida ushbu usullar qo‘llanadi;

- Tarmoq paketlari tarkibidagi matnli va strukturaviy axborotni aniqlash;
- Ma’lumotlarni formatlari orqali aniqlash(karta raqami, identifikatorlar)

Komyuter tarmoqlaridagi konfidensial ma’lumotlarni an’anaviy aniqlash tizimlari asosan oldindan belgilangan shablon va qoidalar asosida ishlaydiz, ammo o‘zgaruvchan va murakkab tarmoq muhitida ushbu metodlar kutilgan natijani bermaydi.Bunga sabab maxfiy axborotlar turli formatda kodlangan yoki fragmentlangan holatda bo‘lishi mumkin.

An’anviy aniqlash usullarining kamchiliklari . Tarmoqdagi konfidentsial trafikni aniqlashning an’anaviy usullari qoida (rule-based) va imzo(signature-based) kabi yondashuvlarga tayanadi. Ushbu usulda aniq va qoidalarga asoslangan kalit so‘zlar, andoza va ma’lumot o‘lchmi kabi atributlar orqali tarmoqdagi axborotni aniqlashga va ajratib olishga harakat qiladi.

Biroq, an’anaviy yondashuvning bir qator kamchiliklari mavjud

- -Ular yangi va o‘zgartirilgan axborotlarni aniqlay olmaydi ya’ni moslashuvchan emas;
- -Oddiy ma’lumotlarni ham muhim deb hisoblashi yokida aksinchga holatlar;
- -Axborot mazmunini hisobga olmaydi;
- -Paketlarga bo‘lingan muhim ma’lumotni aniqlay olmaslik ya’ni fragmentlangan traffik muammosi;

Shuningdek shifrlangan trafik muhim ma’lumotlarni yashirishi mumkin, bu esa zararli faoliyatlarni aniqlash yoki tarmoq tarfigini aniq tasniflashni qiyinlashtiradi.Aynan shu sababdan shifrlangan trafikni tahlil qilish va anomaliyalarni aniqlash uchun statistik usullarni qo‘llash tarmoq xavfsizligini ta’minlashda juda muhimdir [1]

Sun’iy intellekt va uning qo‘llanishi

AI(sun’iy intellekt) tushunchasi mashinalarning inson intellekti bilan bog'liq bo'lgan tabiiy tilni tushunish va qaror qabul qilish kabi vazifalarni bajarish qobiliyatiga ishora qiladi. [1] Sun'iy intellekt (AI) sohasida so‘nggi bir necha o‘n yillikda sezilarli o‘sish kuzatildi, u oddiy tushunchadan turli sohalarda, jumladan tarmoq trafiki tahlilida muhim komponentga aylandi. Ushbu rivojlanish asosiy AI texnologiyalari, masalan, mashina o‘rganish, chuqur o‘rganish va neyron tarmoqlarni rivojlantirish va takomillashtirish bilan xarakterlanadi. Ushbu texnologiyalar tarmoq ma’lumotlarini tahlil qilish, boshqarish va xavfsizligini ta’minlash usullarini tubdan o‘zgartirdi, tarmoq trafigining tobora ortib borayotgan murakkabliklari va hajmlarini hal etdi. [2] [3] [4]

Mashinali o‘rganish (ML) — sun’iy intellektning (AI) bir qismi bo‘lib, ko‘plab ilg‘or AI ilovalari aynan shu asosda yaratiladi. U algoritmlar va statistik modellar yordamida kompyuterlarga aniq ko‘rsatmalarsiz vazifalarni bajarish imkonini beradi, bunda ular andozalar va xulosalar chiqarishga tayanadi. Bu imkoniyat, ayniqsa, tarmoq trafigini tahlil qilishda juda foydalidir, chunki tizim katta hajmdagi ma’lumotlardan o‘rganib, tendensiyalarni aniqlashi, nosozliklarni (anomaliyalarni) aniqlashi va yuzaga kelishi mumkin bo‘lgan muammolarni oldindan bashorat qilishi kerak. [2]

Bundan tashqari, sun’iy intellektning tarmoq trafigini tahlil qilishdagi roli faqat muammolarni aniqlash bilan cheklanib qolmaydi, balki tarmoq samaradorligini optimallashtirishga ham yordam beradi. Masalan, AI asosidagi bashoratli tahlil tarixiy foydalanish andozalariga tayangan holda kelajakdagi tarmoq tirbandligini oldindan aytib berishi mumkin, bu esa tashkilotlarga resurslarni yanada samarali taqsimlash imkonini beradi. Ushbu imkoniyat nafaqat foydalanuvchi tajribasini yaxshilaydi, balki muhim ilovalar uzluksiz ishlashi uchun zarur bo‘lgan tarmoq o‘tkazuvchanligini ham ta’minlaydi. [2, 5]

Mashinali o‘rganish (Machine Learning) asosidagi metodlar. Bu usulda model belgilangan (labelled) ma’lumotlar asosida o‘qitiladi. Bu usulda model belgilangan ma’lumotlar asosida o‘qitiladi.

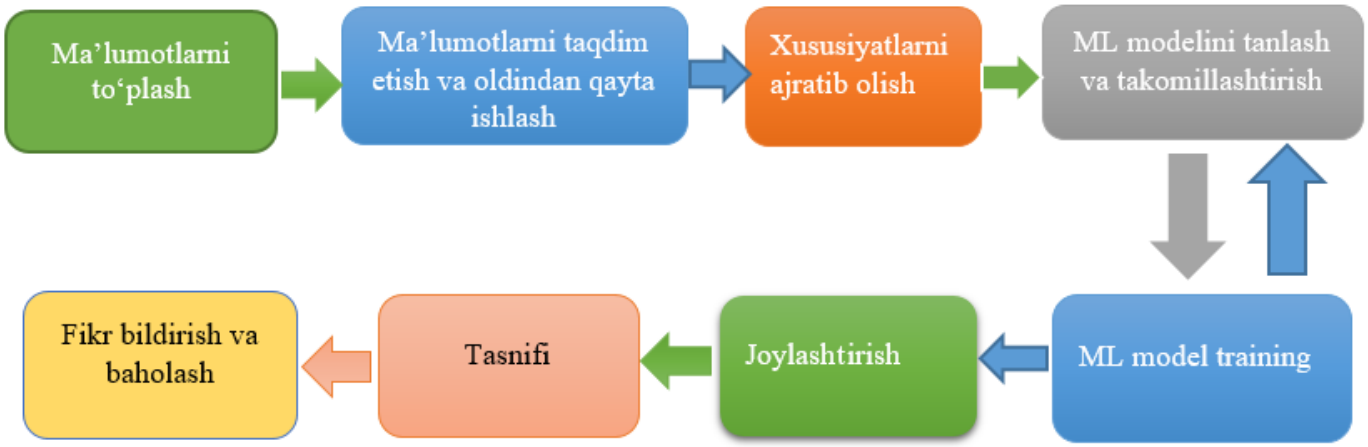
Foydalanishi:

1. -kredit karta raqamlari;
2. -pasport ma’lumotlari;
3. -login va parollar

Mashhur algoritmlar:

- Logistic Regression
- Support Vector Machine (SVM)
- Random Forest
- Naive Bayes [6, 7]

Tarmoq trafigini mashina o‘rganish asosida tasniflash tartibi



Chuqur o‘rganish Deep Learning

Chuqur o‘rganish (Deep Learning) xususiyatlarni (feature) avtomatik ravishda tanlash va o‘rganish qobiliyatiga ega bo‘lib, buning uchun alohida mutaxassis tomonidan ularni tadqiq qilish va tanlash talab etilmaydi. Aynan shu xususiyati tufayli u tarmoq trafigini tasniflash (traffic classification) uchun nihoyatda maqbul yondashuv hisoblanadi. Chuqur o‘rganish an’anaviy mashinali o‘rganish (ML) usullariga nisbatan kengroq o‘rganish imkoniyatiga ega bo‘lib, juda murakkab naqshlarni o‘zlashtira oladi .

Chuqur o‘rganish end-to-end yondashuv sifatida ushbu ikki xususiyatni birlashtirgan holda kirish ma’lumotlari va ularga mos chiqish natijalari o‘rtasidagi nochiziqli bog‘liqlikni o‘rganishga qodir. Shu sababli muammoni xususiyatlarni tanlash va tasniflash kabi kichik kichik masalalarga ajratish zarurati yo‘q. Tarmoq trafigi sohasida keng qo‘llaniladigan chuqur o‘rganish texnikalariga Stacked Self-Encoders (SAE) asosidagi trafik tasniflash usuli, Convolutional Neural Network (CNN) asosidagi trafik tasniflash algoritmi hamda RNN asosidagi trafik tasniflash algoritmi kiradi [8]

Anomaliyani aniqlash. Anomaliya – bu tarmoq xavsizligiga tahdid bo‘lishi mumkin bo‘lgan noodatiy xatti-harakatdir. Nazoratsiz (unsupervised) anomaliya aniqlash usullari tarmoq ma’lumotlarini belgilash (yorliqlash) jarayonining murakkab va qimmatligi, shuningdek, noma’lum hujumlarni aniqlashda nazoratli yoki imzoga asoslangan yechimlarga nisbatan ustunligi sababli tobora ommalashib bormoqda. [9]Suniiy intellect asosidagi IDS va IPS tizimlari aynan shu anomaliyalarni aniqlaydi va tarmoq xavfsizligini ta’minlaydi.

IDS/IPS quyidagi manbalardan ma’lumot oladi:

- -Tarmoq paketlari
- -Log fayllar
- -Server va ilova jurnallari
- -Foydalanuvchi faoliyati
- NIDS – tarmoq darajasida
- HIDS – xost (server/kompyuter) darajasid

Anomaliyalarni aniqlashga mo‘ljallangan boshqa ko‘plab mashinaviy o‘rganish algoritmlari normal **ma’lumotlarning** tavsifini yaratib, ushbu profilga mos kelmaydigan namunalarni anomaliya sifatida aniqlasa, **Isolation Forest** bunday profil yaratmasdan, anomaliyalarni bevosita ajratib oladi (izolyatsiya qiladi). [9]Shuningdek Suniiy intellect oilasiga mansub anomaliyalarni aniqlashda qo‘llaniladigan yana bir tizim **Autoencoder** tizimi hisoblanadi. Avtoenkoderning asosiy vazifasi kirish ma’lumotlarini qayta tiklashdir. Anomaliyalarni aniqlash muammosi sharoitida avtoenkoder normal ma’lumotlarning profilini o‘rganadi, deb taxmin qilinadi. Shuning uchun keyinchalik qayta tiklangan ma’lumotlar (chiqish) bilan asl ma’lumotlar taqqoslanganda, normal holatlarda yo‘qotish (loss) qiymati kichik bo‘ladi, anomaliyalar mavjud bo‘lgan holatlarda esa katta bo‘ladi [10]

Logistic Regression. Logistik regressiya mashinali o'rganishning nazoratli o'rganish yondashuviga asoslangan algoritmlaridan biri bo'lib, u asosan klassifikatsiya masalalarini yechish uchun qo'llaniladi. Ushbu algoritm kirish ma'lumotlari asosida natijaning qaysi kategoriyaga mansubligini aniqlashga xizmat qiladi, ya'ni bashorat qilinadigan qiymat uzluksiz emas, balki diskret bo'ladi.

Logistik regressiya modeli mustaqil o'zgaruvchilar (masalan, daromad darajasi, jamg'arma miqdori yoki kredit tarixi) bilan bog'liq holda ma'lum bir hodisaning yuz berish ehtimolini hisoblaydi va ushbu ehtimol asosida obyektni tegishli sinfga ajratadi. Amaliyotda bu algoritm kredit berish tizimlarida qaror qabul qilish, mijozlarning ishonchliligini baholash hamda boshqa ko'plab iqtisodiy va ijtimoiy sohalarda keng qo'llaniladi.

Kirish ma'lumotlari:

$$X = (x_1 + x_2 \ldots, x_n);$$

Chiziq kombinatsiyasi (Linear model):

$$z = w_0 + w_1 x_1 + w_2 x_2 \ldots., w_n x_n$$

Sigmoid funksiya :

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

Va bog'liq o'zgaruvchi Y faqat ikkilik qiymatga ega 0 yoki 1.

To'liq model teglamasi quyidagi ko'rinishda

$$P(y = 1|x) = \frac{1}{1 + e^{-(w_0 + \sum_{i=1}^{n} w_i x_i}}$$

LSTM (Long Short-Term Memory) arxitekturasi takroran bog'langan kichik tarmoqlar majmuasidan tashkil topgan bo'lib, ular xotira bloklari (memory blocks) deb ataladi. Ushbu xotira bloklari raqamli kompyuterlardagi xotira mikrosxemalarining differensiallanuvchi (differentiable) analogi sifatida qaraladi.

Har bir xotira bloki:

- kamida bitta o'z-o'ziga bog'langan xotira hujayrasidan (memory cell),
- va uchta ko'paytiruvchi mantiqiy birlikdan (multiplicative gates) iborat bo'ladi:
- Input gate (kiritish eshigi),
- Output gate (chiqarish eshigi),
- Forget gate (unutish eshigi).

Mazkur eshiklar mos ravishda yozish (write), o'qish (read) va tozalash (reset) operatsiyalarining uzluksiz (analog) ekvivalentlarini amalga oshiradi.

LSTM (Long Short-Term Memory) algoritmining matematik usulda formulalar bayoni.

Forget gate:

$$f_t = \sigma(W_t[h_{t-1}, x_t] + b_f$$

Bunda:

x_t—t –vaqt bosqichidagi kirish vektori;

h_{t-1} —oldingi yashirin holat;

W_*, b_{t*} —og'irlik va siljitishlar;

σ— sigmoid funksiya ;

Input modulation. Yangi axborotni kiritish darajasini belgilaydi:

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i$$

Nomzod xotira:

$$C_t = tanh(W_c[h_{t-1}, x_t] + b_{fc}$$

Memory cell. Xotira hujayrasini yangilash:

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t)$$

Quyidagi jadvalda turli metodlarning natijalari keltirilgan (simulyatsiya asosida) [11]:

Metod turi	Umumiy aniqlik	Aniqlanganlarning tog'riligi	Aniqlash darajasi	F1-score	FPR
Logistic	78.3	76.1	74.8	75.4	16.9

Regression					
SVM	84.6	83.9	82.1	83.0	11.2
Random Forest	90.9	91.3	89.7	90.5	6.8
Autoencoder	92.7	93.1	92.4	92.7	5.4
CNN	94.2	94.8	93.6	94.2	4.1
LSTM	**95.6**	**96.1**	**95.8**	**95.9**	**3.2**

Mazkur tadqiqot shuni ko‘rsatdiki, kompyuter tarmoqlarida maxfiy ma’lumotlarni aniqlashda sun’iy intellekt asosidagi metodlar an’anaviy yondashuvlarga nisbatan sezilarli darajada foydali hisoblanadi. Ayniqsa, Deep Learning modellari yuqori aniqlik va ishonchlilikni ta’minlaydi. Kelajakdagi tadqiqotlar Federated Learning, Zero Trust Security va AI–Blockchain integratsiyasiga yo‘naltirilishi maqsadga muvofiq.

Foydalanilgan adabiyotlar va internet saytlari

1. M. Paracha, S. Jamil, K. Shahzad, M. Khan va A. L. Rasheed, “AI for Network Threat Detection—A Conceptual Overview.,” Electronics , pp. 13, 4611., 2024-y.
2. J. D. Vraj Shiroya, “Application of AI in Network Traffic,” Artificial Intelligence eJournal, 31-March 2025-Y.
3. A. S. ,. A. T. M Abbasi, “Deep learning for network traffic monitoring and analysis,” Computer Communications, %1-tom170, pp. 19-41, 2021.
4. M. Alom, V. Bontupalli va T. Taha, “Intrusion Detection Using Deep Belief Networks,” %1da In Proceedings of the 2015 National, USA, 2015-y 15-19 June.
5. J. M. S. S. H. Naveed Ahmed, “Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction,” Sensors, p. 22, 2022.
6. J. H. L. M. J. K. W. J. P. S. H. J. J. T. S. Il Hwan Ji, “Artificial Intelligence-Based Anomaly Detection Technology over Encrypted Traffic: A Systematic Literature Review,” Sensors, %1-tom3, p. 898, 2024.
7. N. Sultana, N. Chilamkurti, W. Peng va R. Alhadad, “ Survey on SDN Based Network Intrusion Detection System Using Machine,” Peer-Peer Netw, pp. 493-501, 2019-y.
8. A. Aldweesh, A. Derhab va A. Emam, “Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems: A Survey,,” Knowl.-Based Syst, p. 189, 2020-y.
9. K. F. T.-H. A. V. .. D. Skias, “Network Traffic Anomaly Detection via Deep Learning,” Information, p. 215, 19-May 2021-y.
10. S. S. H. ,. T. S. U. ,. M. R. S. ,. M. A. H. ,. R. M. ,. M. ,. A. M G Abdolrasol, “Artificial neural networks based optimization techniques: A review,” Electronics , p. 21, 2021.
11. M. P. ,. D. H. L. A Kim, “Application of deep learning to real-time Web intrusion detection,” IEEE Access, %1-tom8, pp. 70245-70261, 2020.
12. K. N. ,. G. P. V. ,. O. Z. ,. K. I. ,. F. K. M G Kibria, “Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks,” IEEE access, %1-tom6, 2018.
13. C. C. M. M. Biersack E, “Data traffic monitoring and analysis.,” Lecture Notes in Computer Science, %1-tom5(23), pp. 12561-12570, 2013.
14. Z. Y. C. P. Zhao S, “Network traffic classification using tri-training based on statistical flow characteristics,” IEEE, pp. 323-330, 2017.