

TARMOQ MUHITIDA ANOMAL HOLATLARNI ANIQLASH USULLARI VA REAL VAQT REJIMIDA TARMOQ TRAFIGINI TAHLIL QILISH

Abdusadikov Murodjon Abdukarimovich¹, Fozilov Fayzullo Fatxulla o'g'li²

¹ Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

¹ murodjon1991@icloud.com, ² f.fozilov@tuit.uz

Annotatsiya. Ushbu maqolada tarmoq muhitida yuzaga keladigan anomal holatlarni real vaqt rejimida aniqlash va ularni samarali tahlil qilishga oid zamonaviy yondashuvlar tahlil qilinadi. Tarmoq trafigini onlayn monitoring qilish, zararli faoliyatni aniqlash, kiberxavfsizlik tahdidlariga tezkor javob berish hozirgi kunda IT infratuzilmaning ajralmas qismiga aylangan. Maqolada mashina o'rganish va sun'iy intellekt asosida ishlab chiqilgan modellardan foydalanib, anomal holatlarni avtomatik tarzda aniqlash usullari yoritiladi. Shuningdek, real vaqtli tahlil qilish texnologiyalari, paket darajasida kuzatuv tizimlari va axborot xavfsizligi sohasidagi dolzarb muammolarga e'tibor qaratiladi.

Kalit so'zlar: anomal holatlarni aniqlash, real vaqt rejimi, tarmoq trafigi tahlili, mashina o'qitish, sun'iy intellekt, anomalni asosidagi monitoring, tarmoqni monitoring qilish.

I. KIRISH

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi tarmoq muhitida ma'lumotlar oqimini keskin oshirdi. Shu bilan birga, kibertahdidlar, zararli dasturlar va boshqa xavfli harakatlar soni ham ortmoqda. Anomal holatlarni aniqlash – bu tarmoqda odatdagi faoliyatdan og'ishgan holatlarni aniqlash jarayonidir. Anomal faoliyatlar ko'pincha xakerlik hujumlari, ma'lumotlar sızıntısı yoki DDoS hujumlari bilan bog'liq bo'ladi. An'anaviy signatura asosidagi yondashuvlar ko'pincha yangi tahdidlarni aniqlashda ojizlik qiladi. Shu sababli, zamonaviy tahlil metodlari – ayniqsa mashinali o'rganish, chuqur o'rganish, statistik modellash va gibril yondashuvlar – dolzarb ahamiyat kasb etmoqda [1]. Axborot texnologiyalarining jadal rivojlanishi bilan birga global tarmoqlarga ulanayotgan qurilmalar soni keskin oshdi va tarmoq infratuzilmasi murakkablashib bormoqda. Shu bilan birga, kiberxavfsizlik tahdidlari, zararli dasturiy ta'minotlar, noxush tarmoq trafigi va boshqa turdagi hujumlar soni ham ortib bormoqda. Korxonalar, davlat tashkilotlari va foydalanuvchilar o'z axborot xavfsizligini ta'minlash uchun doimiy ravishda real vaqtli monitoring va nazorat tizimlariga ehtiyoj sezmoqda. Shu nuqtai nazardan anomal holatlarni aniqlash va tahlil qilish zamonaviy tarmoq xavfsizligi strategiyasining eng muhim yo'nalishlaridan biri bo'lib qolmoqda [2].

Ushbu maqolada aynan real vaqt rejimida tarmoq trafigini tahlil qilish, anomaliya asosida hujumlarni aniqlash, zamonaviy algoritmlar va texnologiyalarning qo'llanilishi haqida so'z yuritiladi. Shu bilan birga, mavjud tizimlarning imkoniyatlari, ularning afzalliklari va cheklovlari ham tahlil qilinadi. Tadqiqotlar asosida taqdim etilgan yondashuvlar, ayniqsa, korxona va tashkilotlar uchun samarali tarmoq xavfsizligi strategiyasini ishlab chiqishda foydali bo'lishi mumkin.

II. ASOSIY QISM

Anomal holatlarni aniqlash - bu normal holatdan chetga chiqqan, ya'ni odatdagidan farq qiluvchi tarmoq xatti-harakatlarini aniqlash jarayoni bo'lib, ko'plab kiberhujumlar aynan shu belgilar orqali erta bosqichda aniqlanishi mumkin [3]. An'anaviy statistik usullar bilan bir qatorda hozirda mashina o'rganish (machine learning), sun'iy intellekt (AI) va chuqur o'rganish (deep learning) kabi texnologiyalar bu sohada keng qo'llanilmoqda. Ayniqsa, real vaqt rejimida (real-time) ishlovchi tizimlar tarmoq trafigini doimiy kuzatib, anomal belgilarni aniqlab, operativ chora ko'rishga imkon yaratadi [4].

Tarmoq anomaliyalarini aniqlash - bu kompyuter tarmog'idagi noodatiy naqshlar yoki harakatlarni kuzatish, tahlil qilish va aniqlash uchun ishlatiladigan usul. Bu anomaliyalar odatiy xatti-harakatlardan chetga chiqish bo'lib, ular kiberhujumlar yoki ruxsatsiz kirish kabi potentsial xavfsizlik tahdidlarini ko'rsatishi mumkin. Anomaliyalarni erta aniqlash juda muhim - real vaqtda tarmoqning g'ayritabiiy xatti-harakatlarini aniqlash orqali tashkilotlar xavflarni kamaytirish va tarmoq resurslarini himoya qilish uchun tezda javob berishi mumkin. Haqiqiy vaqtda anomaliyalarni aniqlash tarmoq operatsiyalari (NetOps) va xavfsizlik strategiyalarining muhim tarkibiy qismiga aylandi, bu jamoalarga muammolarni yuzaga kelishi mumkin bo'lgan har qanday zarardan keyin emas, balki sodir bo'lganda aniqlashga yordam beradi. Asosan, tarmoq anomaliyalarini aniqlash oqim yozuvlari, paketlar yoki jurnallar kabi tarmoq telemetriyasi ma'lumotlarini doimiy ravishda to'plashni va ularni oddiy tarmoq xatti-harakatlari bilan taqqoslashni o'z ichiga oladi. Asosiy chiziq tarixiy ma'lumotlar va "oddiy" trafik hajmi, protokollari, IP-manzillari, foydalanuvchilarga kirish shakllari va boshqalar bo'yicha qanday ko'rinishini statistik tahlil qilish yordamida o'rnatiladi. Joriy trafik namunalari ushbu bazaviy chiziqdan sezilarli darajada og'ishsa, tizim tarmoq anomaliyasini belgilaydi.

Raqamli tizimlar tobora ko'proq bir-biriga bog'lanib borayotgan hozirgi zamonda tarmoq xavfsizligi muhim masalaga aylanmoqda. Kiberxavf va hujumlar tobora murakkab tus olmoqda, bu esa an'anaviy xavfsizlik mexanizmlarini yangilashni talab etadi [5]. Anomal holatlarni aniqlash – bu tarmoqdagi odatiy faoliyatdan og'ishgan holatlarni aniqlash jarayonidir. Mashinali o'rganish algoritmlari real vaqtli va murakkab tahdidlarni aniqlash uchun imkoniyat yaratadi.

Ular yordamida tarmoqdagi g'ayritabiiy xatti-harakatlar, zero-day hujumlar va ichki tahdidlar aniqlanishi mumkin (1-rasm).



Statistik usullar



Mashinali o'qitish
algoritmllari



Chuqur o'qitish
yondashuvllari



Gibrid yondashuvlar



Real vaqtli monitoring
tizimllari

1-rasm. Tarmoq muhitida anomal holatlarni aniqlash usullari

- **Statistik usullar.** Statistik usullar anomal holatlarni aniqlashda ma'lumotlarning normal taqsimoti, dispersiyasi, o'rtacha qiymati kabi statistik ko'rsatkichlariga asoslanadi. Bu yondashuvlarda odatdagi (normal) xatti-harakatlar modeli quriladi va ushbu modeldan sezilarli og'ishlar anomaliya sifatida baholanadi. Masalan, Z-score, Mahalanobis masofa, yoki Gaussian Distribution metodlari yordamida tarmoq trafikidagi noodatiy xatti-harakatlar aniqlanadi. Bu usullar soddaligi va tushunariligi bilan ajralib turadi, lekin murakkab yoki o'zgaruvchan muhitlarda samarasiz bo'lishi mumkin.

- **Mashinali o'rganish algoritmllari.** Mashinali o'rganish algoritmllari tarmoq trafigidagi naqshlarni o'rganish va ulardan foydalangan holda yangi anomal holatlarni aniqlashga imkon beradi. Bu yondashuv nazoratli (supervised) va nazoratsiz (unsupervised) shakllarda bo'ladi.

- **Chuqur o'rganish yondashuvllari.** Chuqur o'rganish yondashuvllari sun'iy neyron tarmoqlar (Deep Neural Networks, DNN) yordamida murakkab, yashirin va yuqori o'lchamli naqshlarni aniqlaydi. Ayniqsa Autoencoder, LSTM, va CNN arxitekturalari anomaliya aniqlashda keng qo'llaniladi. Chuqur o'rganish metodlari yuqori samaradorlikka ega, biroq ular katta ma'lumotlar, resurs va murakkab konfiguratsiyani talab qiladi.

- **Gibrid yondashuvlar.** Gibrid yondashuvlar bir nechta texnikani birlashtirgan holda, ularning afzalliklarini jamlaydi va kamchiliklarini bartaraf etishga xizmat qiladi. Gibrid usullar orqali bir metod statistik filtrlashni amalga

oshiradi, boshqasi esa chuqur tahlil qiladi. Bunday yondashuvlar ko‘p qatlamli tarmoq xavfsizligi tizimlarida qo‘llanadi.

- **Real vaqtli monitoring tizimlari.** Real vaqtli monitoring tizimlari tarmoq trafiginii uzluksiz tarzda tahlil qilib, anomal holatlarni darhol aniqlash va ogohlantirish imkonini beradi. Bu tizimlar anomaliyani aniqlovchi model bilan integratsiyalashgan bo‘lib, xavfni real vaqtda aniqlash, vizualizatsiya qilish va javob berish imkoniyatini yaratadi. Ular yuqori samaradorlikka ega bo‘lsa-da, katta resurs va optimallashtirilgan konfiguratsiyalarni talab qiladi.

Internet xizmatlarining ko‘payishi, bulut texnologiyalari va IoT qurilmalarining keng tarqalishi tarmoqda harakatlanuvchi ma’lumotlar hajmining keskin oshishiga olib kelmoqda. Bu esa nafaqat tarmoq samaradorligi, balki uning xavfsizligi va ishonchliligiga ham jiddiy talablar qo‘yadi. Shuning uchun axborot oqimini doimiy nazorat qilish, ehtimoliy hujumlarni oldindan aniqlash, hamda tarmoq faoliyatidagi anomal belgilarni erta bosqichda aniqlab, xavfli holatlarning oldini olish maqsadida real vaqtli tarmoq trafiginii tahlil qilish alohida ahamiyat kasb etadi. Bu tahlil axborot xavfsizligini ta’minlashda, xizmatlar uzluksizligini saqlashda va tarmoq resurslaridan samarali foydalanishda muhim vosita sifatida namoyon bo‘lmoqda. Hozirgi vaqtda tarmoq trafiginii real vaqt rejimida tahlil qilish uchun bir nechta samarali va ilg‘or yondashuvlar mavjud. Bu usullar tarmoqda sodir bo‘layotgan harakatlarni tezkor aniqlash, xavfsizlik tahdidlarini erta bosqichda aniqlash hamda tarmoq holati haqida to‘liq tasavvurga ega bo‘lish imkonini beradi. Har bir yondashuv o‘ziga xos metodologiyasi, texnik imkoniyatlari va qo‘llanish sohalariga ega bo‘lib, ular tarmoq infratuzilmasining murakkabligiga qarab tanlanadi yoki birgalikda qo‘llaniladi. Ayniqsa, bugungi kunda axborot xavfsizligiga bo‘lgan talablar ortib borayotgan bir sharoitda, bu usullarning har birini chuqur o‘rganish va amaliyotda qo‘llash dolzarb ahamiyat kasb etmoqda [6]. Real vaqtli tahlil usullari orqali foydalanuvchilarning noodatij xatti-harakatlari aniqlanishi, zararli dasturlar tarqalishining oldi olinishi, xizmatga hujum (DDoS), port skanerlash, manzillarning qalbakilashtirilishi (spoofing) kabi ko‘plab tahdidlar darhol aniqlanishi mumkin. Bundan tashqari, monitoring natijalari asosida tarmoq siyosatlarini optimallashtirish, xavfsizlik devorlarini sozlash va foydalanuvchi faoliyatini tartibga solish ham mumkin bo‘ladi. Quyida biz ushbu yondashuvlarning asosiylarini texnik va amaliy nuqtayi nazardan batafsil ko‘rib chiqamiz:

- **Paket darajasida monitoring:** har bir kelayotgan yoki ketayotgan tarmoq paketining strukturasi, manzili va mazmuni tahlil qilinadi.

- **Flow-based analiz:** tarmoq oqimlari (flows) asosida tahlil, bu NetFlow, sFlow kabi protokollar orqali amalga oshiriladi.

- **Anomaliyani aniqlash:** mashinaviy o‘rganish (machine learning) asosida normal va anomal xatti-harakatlarni ajratish.

▪ **Signaturaga asoslangan aniqlash:** IDS (masalan, Snort, Suricata) orqali oldindan ma'lum bo'lgan hujumlar signaturalari asosida tahdidlarni aniqlash.

Tarmoq trafigini real vaqt rejimida tahlil qilishda tizim resurslarining samarali ishlatilishi, monitoring vositalarining kengaytiriluvchanligi va tahlilning aniqligi muhim omillar hisoblanadi [7]. Suricata va Zeek kabi vositalar tarmoq trafigini chuqur tahlil qilishda ustunlikka ega, biroq ularni sozlash murakkab va tajribani talab qiladi. Mashinaviy o'rganish asosidagi tizimlar esa yangi, ilgari noma'lum bo'lgan tahdidlarni aniqlash imkonini beradi [8]. Monitoring tizimlari o'rnatilgan real tarmoq muhitida olib borilgan eksperimentlar bir necha bosqichda tashkil etiladi [9]. Dastlab, tarmoq muhiti simulyatsiya qilindi va ma'lum trafik ssenariylari (masalan, oddiy foydalanuvchi faoliyati, DDoS, port skanerlash) sun'iy ravishda generatsiya qilindi. Shundan so'ng Wireshark, Zeek, ntopng va Suricata monitoring vositalari yordamida ushbu trafiklar real vaqt rejimida tahlil qilindi. Har bir vosita tomonidan aniqlangan tahdidlar soni, aniqlik darajasi, soxta musbat (false positive) va soxta manfiy (false negative) ko'rsatkichlar qayd etildi. Quyida keltirilgan jadval turli real vaqtli tarmoq monitoring vositalarining samaradorligini aniqlik, soxta musbat va soxta manfiy ko'rsatkichlari asosida taqqoslaydi. Ushbu vositalar asosida olib borilgan tahlillar orqali ularning amaliy jihatdan afzalliklari va cheklovlari aniqlangan (1-jadval).

1-jadval. Real vaqtli monitoring vositalarining samaradorlik taqqoslamasi

Vosita	Aniqlik (%)	Soxta Musbat (%)	Soxta Manfiy (%)	Afzalliklari
Zeek	95.2	2.1	2.7	Kengaytirilgan tahlil, foydalanuvchi skriptlar
Suricata	96.7	1.8	1.5	Yaxshi signatura asosli aniqlash, JSON chiqish
Wireshark	90.5	4.5	5.0	Tarmoq diagnostikasi uchun batafsil ko'rinish
ntopng	89.1	3.9	7.0	Vizual interfeys, statistik ko'rsatkichlar
RNN Modeli	92.8	2.4	4.8	Sekvensiyal anomaliyani aniqlash
Isolation Forest	91.3	3.1	5.6	Anomaliyaga sezgirlik, ishlov tezligi

Ushbu jadval tarmoq monitoring vositalari va mashinaviy o'rganishga asoslangan modellarni turli ko'rsatkichlar bo'yicha taqqoslaydi. Natijalar shuni

ko'rsatadiki, an'anaviy monitoring vositalari, ayniqsa Suricata va Zeek signatura asosli tahlil orqali aniqlik darajasi bo'yicha yetakchi o'rinda turadi. Suricata, ayniqsa, juda past soxta musbat va soxta manfiy ko'rsatkichlarga ega bo'lib, hujumlarni aniqlashda eng ishonchli vosita sifatida ajralib turdi. Zeek esa foydalanuvchiga moslashtirish imkoniyatlari bilan ajralib turadi. Mashinaviy o'rganishga asoslangan modellar (RNN va Isolation Forest) esa, ayniqsa yangi, ilgari noma'lum tahdidlarni aniqlashda foydali bo'lib, ularning samaradorligi real holatlarda yuqori bo'lishi mumkin. Ular signatura asosidagi tizimlarga qaraganda yanada moslashuvchan, lekin ularni o'qitish va sozlash ko'proq resurs va vaqt talab qiladi.

Tarmoq muhitida anomal holatlarni aniqlash uchun mashinali o'qitish yondashuvlari keng qo'llanilmoqda. Ushbu usullar tarmoq trafikidagi g'ayritabiiy xatti-harakatlarni avtomatik tarzda aniqlash, baholash va oldini olish imkonini beradi. Mashinali o'qitish usullari statistik naqshlar, vaqtli bog'liqliklar va yashirin xususiyatlar orqali anomalialarni yuqori aniqlikda aniqlay oladi.

- *Support Vector Machines (SVM).* Support Vector Machine — bu klassifikatsiya uchun mo'ljallangan kuchli nazoratli o'rganish algoritmi. Uning vazifasi — ma'lumotlar to'plamidagi turli sinflarni maksimal ajratuvchi gipertekislikni aniqlash. Anomaliya aniqlashda SVM tarmoq trafiklarini “normal” va “shubhali” deb ajratishga xizmat qiladi.

- *Random Forest.* Random Forest – bu bir nechta qaror daraxtlari (Decision Trees) yig'indisiga asoslangan klassifikatsiya algoritmi bo'lib, har bir daraxt mustaqil qaror qabul qiladi va ularning ko'pchilik fikri asosida yakuniy natija aniqlanadi. Bu usul tarmoqdagi murakkab va xilma-xil hujumlarni aniqlashda foydalidir.

- *K-means klasterlash.* K-means – bu nazoratsiz o'rganish algoritmi bo'lib, ma'lumotlarni o'xshashlik asosida bir nechta klasterlarga ajratadi. Anomalialar bu klasterlardan uzoq joylashgan nuqtalar sifatida aniqlanadi. Bu yondashuv oldindan belgilangan sinf yorliqlarini talab qilmaydi.

- *DBSCAN (Density-Based Spatial Clustering of Applications with Noise).* DBSCAN – zichlik asosida ishlovchi klasterlash algoritmidir. Bu metod ma'lumotlarni zichligi asosida guruhlaydi va siyrak joylashgan nuqtalarni anomaliya deb belgilaydi. Tarmoq xavfsizligida kam uchraydigan, ammo xavfli xatti-harakatlarni aniqlashda ayniqsa foydalidir.

- *Neyron tarmoqlar (Neural Networks).* Neyron tarmoqlar – inson miyasi faoliyatini model qiluvchi algoritmlar bo'lib, murakkab naqsh va bog'liqliklarni aniqlay oladi. Ular an'anaviy algoritmlar aniqlay olmaydigan yashirin xususiyatlarni o'rganishda foydalidir.

- *Autoencoder.* Autoencoder — chuqur o'rganishga asoslangan neyron tarmoq bo'lib, kiruvchi ma'lumotni siqilgan shaklga aylantirib, uni asl holatiga

qaytarishga harakat qiladi. Agar qayta tiklanishdagi xatolik yuqori bo'lsa, bu anomaliya sifatida belgilanadi.

- *LSTM (Long Short-Term Memory)*. LSTM – vaqt ketma-ketligi bilan ishlovchi neyron tarmoq bo'lib, tarmoq trafiklarining vaqtli bog'liqligini aniqlashda qo'llaniladi. U uzoq vaqtdagi kontekstni saqlab qolish xususiyatiga ega.

- *Gibrid yondashuvlar (Hybrid Approaches)*. Gibrid yondashuvlar bir nechta algoritmlarning kuchli jihatlarini birlashtiradi. Masalan, SVM nazoratli yondashuv sifatida ishlatiladi, Autoencoder esa nazoratsiz shaklda yordamchi sifatida qo'shiladi. Bu metodlar murakkab va noaniq holatlarni aniqlashda yuqori samaradorlik beradi.

Tadqiqot davomida bir nechta mashinali o'qitish yondashuvlari asosida tarmoq muhitida anomal holatlarni aniqlash samaradorligi tajriba yo'li bilan baholandi. Baholash jarayonida aniqlik (Accuracy), F1-score va ishlash vaqti kabi mezonlardan foydalanildi. Quyidagi 2-jadvalda anomal holatlarni aniqlashda ba'zo mashinali o'qitish usullarining taqqoslamali samaradorligi keltirilgan.

2-jadval. Tarmoq muhitida anomal holatlarni aniqlashda mashinali o'qitish usullarining samaradorlik ko'rsatkichlari

Usul	Aniqlik (Accuracy)	F1-score	Ishlash vaqti
Decision Tree	89%	0.87	Tez
SVM	91%	0.89	O'rtacha
Autoencoder	94%	0.92	Sekin
LSTM	96%	0.94	Sekinroq
Gibrid Model	97%	0.95	O'rtacha

Natijalar shuni ko'rsatadiki, gibrid model barcha mezonlar bo'yicha eng yuqori samaradorlikni namoyon qildi. Ayniqsa aniqlik va F1-score ko'rsatkichlari bo'yicha bu model boshqa yondashuvlardan ustun bo'ldi. Chuqur o'qitish asosidagi LSTM model ham yuqori aniqlikni ko'rsatgan bo'lsa-da, uning ishlash tezligi nisbatan past bo'ldi. Autoencoder modelida aniqlik yuqori bo'lishiga qaramasdan, uni o'qitish uchun ko'proq vaqt talab qilindi. SVM va Decision Tree esa o'rtacha samaradorlik ko'rsatib, real vaqtli yoki cheklangan resursli muhitlar uchun mos bo'lishi mumkin. Umuman olganda, aniqlik va samaradorlik o'rtasidagi muvozanatni saqlab qolish uchun gibrid yondashuvlar eng optimal tanlov sifatida ko'rilmogda.

III. XULOSA

Yuqoridagi tadqiqotlar shuni ko'rsatadiki, tarmoq xavfsizligini ta'minlashda real vaqt rejimida anomal holatlarni aniqlash va tahlil qilish muhim strategik ahamiyat kasb etadi. Gibrid yondashuvlar, ayniqsa, aniqlik va samaradorlik o'rtasidagi muvozanatni ta'minlab bera oladigan eng optimal yechim sifatida ajralib turadi. Mashinaviy o'rganish asosidagi modellar, xususan, LSTM va Autoencoder yuqori aniqlikka ega bo'lsa-da, ularning ishlash tezligi va o'qitish talablari real vaqtli tizimlar uchun har doim mos kelavermaydi. Shu bois, gibrid modellarning samaradorligi, aniqligi va ishlash barqarorligi bunday muhitlar uchun juda muhim omil hisoblanadi. Bundan tashqari, Suricata va Zeek kabi tarmoq monitoringi vositalarining integratsiyasi orqali yanada kompleks va ko'p qatlamli himoya tizimlari shakllantiriladi. Bu vositalar mashinaviy o'rganish modellari bilan uyg'unlashgan holda ishlatilsa, nafaqat mavjud tahdidlarni aniqlash, balki yangi, ilgari uchramagan hujumlarni ham prognoz qilish imkoniyati yaratiladi. Tarmoq trafiginin real vaqt rejimida tahlil qilish, aniqlik, tezkorlik va moslashuvchanlikni birlashtirgan holda, zamonaviy kiberxavfsizlik sohasida yetakchi yondashuv sifatida namoyon bo'lmoqda.

FOYDALANILGAN ADABIYOTLAR

1. Shamshari, Alqasim & Najaf, Habiba & Hussain, Shafiq. (2024). Machine Learning Approaches for Anomaly Detection in Network Security.
2. Xaydaraliyev Elbek Farxod O'G'Li (2024). "Raqamli iqtisodiyotda axborot xavfsizligini ta'minlashning zamonaviy usullari va vositalari". Central Asian Journal of Education and Innovation, 3 (11), 58-63. doi:10.5281/zenodo.14059286.
3. "Network Anomaly Detection: A Comprehensive Guide". Kentik, 14 Mar. 2025, <https://www.kentik.com/kentipedia/network-anomaly-detection/>.
4. Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: A machine learning perspective. CRC Press.
5. Shon, T., & Moon, J. (2007). A hybrid machine learning approach to network anomaly detection. Information Sciences, 177(18), 3799–3821.
6. Jakkani, Anil. (2024). Real-Time Network Traffic Analysis and Anomaly Detection to Enhance Network Security and Performance: Machine Learning Approaches. Journal of Electronics Computer Networking and Applied Mathematics. 4. 2799-1156. 10.55529/jecnam.44.32.44.
7. Inc, Stamus Networks, "Suricata vs Zeek," Stamus Networks. [Online]. Available: <https://www.stamus-networks.com/suricata-vs-zeek>.
8. M. A. Wahed, "Real-Time Intrusion Detection and Traffic Analysis Using AI Techniques in IoT Infrastructure," 2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI), Sana'a, Yemen, 2024, pp. 1-6, doi: 10.1109/ICETI63946.2024.10777213.



9. Ogogo, Wycliffe. (2021). Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security. East African Journal of Information Technology. 3. 1-6. 10.37284/eajit.3.1.153.