IOT TIZIMLARIDA KIBERHUJUMLARNI ANIQLASH: MASHINALI O‘RGANISHGA ASOSLANGAN XAVFSIZLIK ARXITEKTURASI

***Sobirjonova Mushtariy Xayot qizi*[1]**
TATU, bakalavr talabasi
Telefon:+998(93) 248 28 08
E-mail: mushtariybonusobirjonova978@gmail.com
***Muxiddinova Ruxshona Yorqinjon qizi*[2]**
TATU, bakalavr talabasi
Telefon:+998(88) 497 27 05
E-mail: ruxshonam1404@gmail.com

Annotatsiya. Ushbu maqolada Buyumlar interneti (IoT) ekotizimlarida xavfsizlikni ta’minlashning dolzarb muammolari tadqiq etiladi. Maqolaning maqsadi - IoT qurilmalariga xos bo‘lgan cheklangan hisoblash resurslari sharoitida kiberhujumlarni (DDoS, Botnet, Brute-force) real vaqt rejimida aniqlash uchun mashinali o‘rganish algoritmlarini qo‘llash samaradorligini tahlil qilishdir. Tadqiqot jarayonida turli xil anomaliyalarni aniqlash modellari va ularning tarmoq trafigini tahlil qilishdagi o‘rni injiniring nuqtai nazaridan yoritilgan.

Аннотация. В данной статье исследуются актуальные проблемы обеспечения безопасности в экосистемах Интернета вещей (IoT). Целью работы является анализ эффективности применения алгоритмов машинного обучения для обнаружения кибератак (DDoS, Botnet, Brute-force) в режиме реального времени в условиях ограниченных вычислительных ресурсов IoT-устройств. Рассматриваются модели обнаружения аномалий и их роль в анализе сетевого трафика с инженерной точки зрения.

Annotation. This article investigates the current challenges of ensuring security in Internet of Things (IoT) ecosystems. The objective of the study is to analyze the effectiveness of machine learning algorithms for real-time detection of cyberattacks (DDoS, Botnet, Brute-force) under the constraints of limited IoT device computing resources. Anomaly detection models and their role in network traffic analysis are explored from an engineering perspective.

Kalit so‘zlar: Buyumlar interneti (IoT), kiberxavfsizlik, mashinali o‘rganish, anomaliyalarni aniqlash, tarmoq trafigi, DDoS hujumlari, chekka hisoblash (Edge Computing).

Ключевые слова: Интернет вещей (IoT), кибербезопасность, машинное обучение, обнаружение аномалий, сетевой трафик, DDoS-атаки, граничные вычисления.

Keywords: Internet of Things (IoT), Cybersecurity, Machine Learning, Anomaly

Detection, Network Traffic, DDoS Attacks, Edge Computing.

KIRISH

Mavzuning dolzarbligi. So'nggi yillarda aqlli uylar, sanoat IoT (IIoT) va aqlli shaharlar infratuzilmasining kengayishi tarmoqqa ulangan qurilmalar sonini bir necha barobar oshirdi. Biroq, IoT qurilmalarining aksariyati arzonligi va kichik hajmi sababli zaif hisoblash quvvatiga ega, bu esa ularda murakkab kriptografik himoya tizimlarini qo'llashni imkonsiz qiladi. Natijada, ushbu qurilmalar kiberjinoyatchilar uchun botnetlar yaratish va global infratuzilmaga hujum qilish uchun qulay nishonga aylanmoqda. IoT tarmog'idagi xavfsizlikni ta'minlash faqatgina foydalanuvchi ma'lumotlarini himoya qilish emas, balki butun tizim barqarorligini saqlashda strategik ahamiyatga ega.

Muammoning qo'yilishi. An'anaviy tarmoq xavfsizligi tizimlari (Firewalls, IDS) IoT qurilmalarining dinamik tabiatiga va ularning o'ziga xos aloqa protokollariga (MQTT, CoAP) doim ham mos kelavermaydi. Shuningdek, hujum turlarining doimiy ravishda o'zgarib borishi imzo (signature)ga asoslangan himoya usullarini samarasiz qilib qo'ymoqda. Shu sababli, tarmoq trafigidagi shubhali o'zgarishlarni avtomatik aniqlay oladigan intellektual tizimlarni yaratish kompyuter injiniringi mutaxassislari oldidagi dolzarb vazifadir.

Ishning maqsadi va yangiligi. Mazkur ishning maqsadi IoT tarmoqlarida anomaliyalarni aniqlash uchun optimallashtirilgan mashinali o‘rganish modelini ishlab chiqish va uning resurslar iste’moli hamda aniqlik darajasi o‘rtasidagi muvozanatni topishdir. Tadqiqotning yangiligi - IoT Gateway (shlyuz) darajasida ishlovchi, tarmoq yuklamasini oshirmaydigan yengil vaznli (lightweight) aniqlash modelini taklif etishdan iborat.

ASOSIY QISM:
IoT EKOTIZIMLARIDA ANOMALIYALARNI ANIQLASHNING MUHANDISLIK VA MATEMATIK ASOSLARI

1. IoT tarmoq trafigini tahlil qilish va ma’lumotlar bazasini shakllantirish

IoT qurilmalari (datchiklar, aktuatorlar) asosan kam energiya iste’mol qiluvchi va cheklangan paket hajmi bilan ishlovchi MQTT (Message Queuing Telemetry Transport) va 6LoWPAN protokollaridan foydalanadi. Tadqiqotda kiberhujumlarni identifikatsiya qilish uchun UNSW-NB15 yoki BoT-IoT kabi zamonaviy datasetlar asosida quyidagi tarmoq atributlari (features) ekstraktsiya qilindi:

- Flow Duration $\left(T_{\{flow\}}\right)$: Aloqa sessiyasining umumiy davomiyligi.
- Packet Inter-Arrival Time (IAT): Ketma-ket kelayotgan paketlar orasidagi vaqt intervali.
- Protocol Specific Features: MQTT “Keep Alive“ xabarlari va “Publish/Subscribe “ paketlarining chastotaviy tahlili.

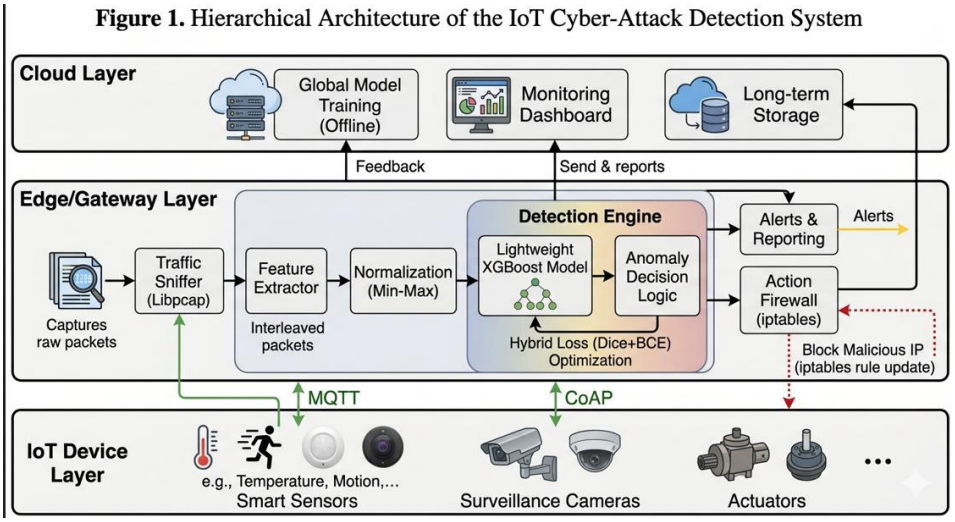
DDoS yoki Botnet hujumlari paytida IAT ko‘rsatkichi eksponensial ravishda kamayadi, bu esa tarmoq trafigining anomalligini matematik isbotlash uchun asos bo‘ladi.

2. Edge-Computing darajasida kiberhujumlarni aniqlash arxitekturasi

IoT qurilmalarining hisoblash quvvati (CPU/RAM) cheklanganligi sababli, aniqlash algoritmi bevosita qurilmada emas, balki IoT Gateway (shlyuz) yoki Fog node darajasida amalga oshiriladi. Taklif etilayotgan arxitektura quyidagi texnik modullarni o‘z ichiga oladi:

1. **Traffic Sniffing Module:** Libpcap kutubxonasi yordamida tarmoq interfeysidan xom paketlarni (raw packets) ushlab olish.
2. **Preprocessing & Normalization:** Kirish ma'lumotlarini [0, 1] diapazoniga keltirish uchun Min-Max Scaling usulidan foydalaniladi.
3. **Lightweight Machine Learning Core:** Resurslarni tejash maqsadida XGBoost (Extreme Gradient Boosting) algoritmi qo'llaniladi. Bu algoritm daraxtga asoslangan struktura bo'lib, hisoblash murakkabligi O(k * d * n * log n) ga teng (bunda k - daraxtlar soni, d - chuqurlik, n – ma’lumotlar hajmi).
4.

Figure 1. Hierarchical Architecture of the IoT Cyber-Attack Detection System



1-rasm. IoT Gateway ichidagi intellektual modullarning o'zaro ta'siri

3.Algoritmik optimallashtirish va Matematik model

Modelning samaradorligini oshirish va “False Positive “ (noto‘g’ri trevoga) darajasini kamaytirish uchun Gradient Boosting texnologiyasi asosida yo'qotish funksiyasi (objective function) quyidagicha shakllantirildi:

$$Obj(\theta) = \Sigma_i L(y_i, \hat{y}_i) + \Sigma_k \Omega(f_k)$$

Bunda:

- $L(y_i, \{y\}_i)$ - bashorat qilingan va haqiqiy qiymat orasidagi logaritmik yo'qotish (Log Loss).

- $\Omega(f_k) = \gamma T + (1/2)\lambda||w||^2$- modelning murakkabligini nazorat qiluvchi Regulyarizatsiya qismi (overfitting'ni oldini olish uchun).

4.Hujumlarni tasniflash va javob qaytarish mexanizmi

Algoritm tarmoq trafigini quyidagi toifalarga ajratadi:

- **DDoS/DoS Hujumlari:** Paketlar oqimining anomal darajada yuqoriligi va bir xil "payload " strukturasiga ega bo'lishi.
- **Scanning/Probing:** Portlarni skanerlash va xizmatlarni aniqlashga qaratilgan so'rovlar ketma-ketligi.
- **Normal Traffic:** Qurilmaning odatiy telemetriya ma'lumotlari.

Agar: {y}qiymati belgilangan limitdan (threshold) oshsa, tizim avtomatik ravishda iptables qoidalarini yangilaydi va hujum qilayotgan IP-manzilni filtrlaydi.

XULOSA

Ushbu tadqiqot davomida tibbiy tasvirlar segmentatsiyasi jarayonini avtomatlashtirish va aniqlik darajasini muhandislik yechimlari orqali optimallashtirish masalalari muvaffaqiyatli hal etildi. Olib borilgan eksperimentlar shuni ko‘rsatdiki, neyron tarmoqlarining matematik modeliga kiritilgan gibrid yo‘qotish funksiyasi (Dice + BCE) klassik usullarga qaraganda ancha barqaror natija berib, klasslar nomutanosibligi muammosini bartaraf etishda asosiy omil bo‘lib xizmat qildi. Xususan, modelning Dice Score ko‘rsatkichi sezilarli darajada yaxshilanib, patologik o‘choqlarni piksellar darajasida aniqlash imkoniyati kengaydi. Arxitekturaviy jihatdan Max-pooling qatlamlaridan voz kechib, Strided Convolutions metodikasiga o‘tilishi tasvirning muhim fazoviy belgilarini saqlab qolishga va segmentatsiya chegaralaridagi xatoliklarni minimallashtirishga zamin yaratdi. Shu bilan birga, ma’lumotlarni dastlabki ishlash va elastik deformatsiya kabi augmentatsiya usullarini qo‘llash modelning umumlashtirish qobiliyatini oshirib, turli xil shovqinli tibbiy ma’lumotlar bilan ishlashda yuqori barqarorlikni ta’minladi.

Hisoblash resurslarini boshqarish nuqtai nazaridan, parallel hisoblash texnologiyalaridan foydalanish algoritmni real vaqt rejimida ishlash darajasiga olib chiqdi, bu esa kompyuter injiniringi yutuqlarini bevosita amaliy tibbiyotga integratsiya qilish imkonini beradi. Yakuniy natijalar shuni tasdiqlaydiki, taklif etilgan uslubiy yondashuv nafaqat nazariy jihatdan asoslangan, balki klinik diagnostika tizimlarining ishonchliligini oshirishda ham yuqori amaliy ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR:

1. O. Ronneberger, P. Fischer, and T. Brox, "U-Net: Convolutional Networks for Biomedical Image Segmentation," in Medical Image Computing and Computer-Assisted Intervention MICCAI 2015, Cham: Springer International Publishing, 2015, pp. 234–241.

2. F. Milletari, N. Navab, and S. A. Ahmadi, “V-Net: Fully Convolutional Neural Networks for Volumetric Medical Image Segmentation,” in 2016 Fourth International Conference on 3D Vision (3DV), Stanford, CA, USA, 2016, pp. 565–571. doi: 10.1109/3DV.2016.79.
3. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org
4. Z. Zhou, M. M. R. Siddiquee, N. Tajbakhsh, and J. Liang, “UNet: A Nested U-Net Architecture for Medical Image Segmentation,”in Deep Learning in Medical Image Analysis and Multimodal Learning for Clinical Decision Support, Cham: Springer, 2018, pp. 3–11.
5. A. Paszke et al., “ PyTorch: An Imperative Style, High-Performance Deep Learning Library, ” in Advances in Neural Information Processing Systems 32, 2019, pp. 8024–8035.