IOTGA ASOSLANGAN ZARARLI DASTURLARNI ANIQLASH MODEL VA ALGORITMLARI

Abdumalikov Akmaljon Abduxoliq o'g'li[1],*Qodirova Laylo Sobir qizi*[2]

[1]*Mirzo Ulug'bek nomidagi O'zMU Jizzax filiali dotsenti*
[2]*Mirzo Ulug'bek nomidagi O'zMU Jizzax filiali magistranti*
E-mail: akmalabdumalikov6@gmail.com layloinomova9@gmail.com

K E Y W O R D S

IoT xavfsizligi, zararli dasturlar, malware aniqlash, XGBoost, genetika algoritmi, gibrid model

A B S T R A C T

Ushbu maqola IoT tizimlarida zararli dasturlarni aniqlash uchun yangi gibrid xavfsizlik model va algoritmlarini taklif etadi. Zararli dasturlarning mohiyati, turlari (viruslar, troyanlar, ransomware, botnetlar) va IoTga ta'sirini tahlil qilib, mavjud aniqlash usullarining cheklovlari aniqlandi. Taklif etilgan model XGBoost algoritmini genetika algoritmi bilan birlashtirishga asoslanadi va IoT qurilmalarida real vaqt rejimida ishlay olishi uchun engil vaznli komponentlardan iborat. Maqola natijalari IoT tarmoqlarida xavfsizlikni ta'minlashning yangi, samarali yo'nalishini ochib beradi.

Zamonaviy raqamli muhitda Internet of Things (IoT) tizimlari hayotning turli jabhalarida, jumladan, aqlli shaharlar, tibbiyot, sanoat va uy xo'jaligida keng tarqalmoqda. IoT qurilmalari sonining tez o'sishi – 2025 yilga kelib 75 milliarddan ortiq qurilma bo'lishi taxmin qilinmoqda – bu tarmoqlarning xavfsizligiga jiddiy tahdidlar keltirib chiqarmoqda. Zararli dasturlar IoT ekotizimiga kirib borib, ma'lumotlar o'g'irlashi, DDoS hujumlarini amalga oshirishi yoki butun tarmoqni buzishi mumkin. Zararli dasturlar mohiyati jihatidan yashirin kodlar bo'lib, ular qurilmalarga ruxsatsiz kirib, normal ishlashini buzadi, resurslarni o'z manfaatlariga ishlatadi yoki ma'lumotlarni shifrlaydi. Bu muammo IoT qurilmalarining cheklangan resurslari energiya, xotira va hisoblash quvvati tufayli yanada murakkablashadi, chunki an'anaviy antivirus dasturlari bu qurilmalarda samarali ishlamaydi.

IoT tarmoqlarida zararli dasturlarning tarqalishi global miqyosda dolzarb muammo hisoblanadi. Zararli dasturlarning turlari bo'yicha tahlil qilganda, ularni quyidagi asosiy kategoriyalarga ajratish mumkin: viruslar o'zini ko'paytiruvchi kodlar, troyanlar -yashirin kiruvchi dasturlar, ransomware-ma'lumotlarni shifrlovchi va to'lov talab qiluvchi, botnetlar-qurilmalarni masofadan boshqaruvchi tarmoqlar va wormlar tarmoq orqali tarqaluvchi. IoT kontekstida botnetlar, masalan Mirai turi, eng katta tahdid bo'lib, ular qurilmalarni DDoS hujumlariga ishlatadi. Bu turlar IoTning zaifliklarini (standart parollar, yangilanmagan dasturiy ta'minot) foydalanib, tez tarqaladi va aniqlashni qiyinlashtiradi.

Adabiyotlar sharhiga ko'ra, zararli dasturlarni aniqlashning an'anaviy usullari, masalan signature-based yondashuvlar, yangi mutatsiyalarga qarshi samarasiz bo'lib qolmoqda. So'nggi tadqiqotlarda mashina o'rganishiga asoslangan modellar, jumladan CNN va LSTM gibrid tizimlari, IoTda zararli dasturlarni aniqlashda 90% dan yuqori aniqlik ko'rsatgan. Biroq, bu modellar katta ma'lumotlar to'plamlarini talab qiladi va resurs cheklangan IoT qurilmalarida real vaqtda ishlamaydi. Boshqa ishda GRU-CNN gibrid modeli IoT xavfsizligini yaxshilash uchun taklif etilgan bo'lib, u anomaliyalarni tez aniqlaydi, lekin federated learning integratsiyasi yetishmaydi. Yana bir tadqiqotda engil vaznli mashina o'rganishi algoritmlari IoT malware aniqlash uchun qo'llanilgan, ammo ularning samaradorligi faqat laboratoriya sharoitida sinovdan o'tkazilgan. Umumiy kamchilik sifatida, mavjud modellar zararli dasturlarning dinamik tabiatini to'liq hisobga olmaydi va IoT protokollariga moslashmagan. Ushbu maqolaning maqsadi zararli dasturlarni aniqlovchi IoTga asoslangan mavjud xavfsizlik model va algoritmlarini tahlil qilishdan iborat.

©A.A. Abdumalikov, L.S. Qodirova

Zararli dasturlar ya’ni malware mohiyati jihatidan kompyuter tizimlariga yashirin ravishda kirib boruvchi va zarar yetkazuvchi dasturiy kodlar bo'lib, ular qurilmalarning normal ishlashini buzadi, ma’lumotlarni o'g'irlaydi yoki resurslarni masofadan boshqaradi. IoT kontekstida bu dasturlar qurilmalarning cheklangan quvvati va tarmoq bog'lanishini foydalanib, katta miqyosli hujumlar tashkil etadi. Zararli dasturlarni tahlil qilish statik va dinamik usullarga bo‘linadi.

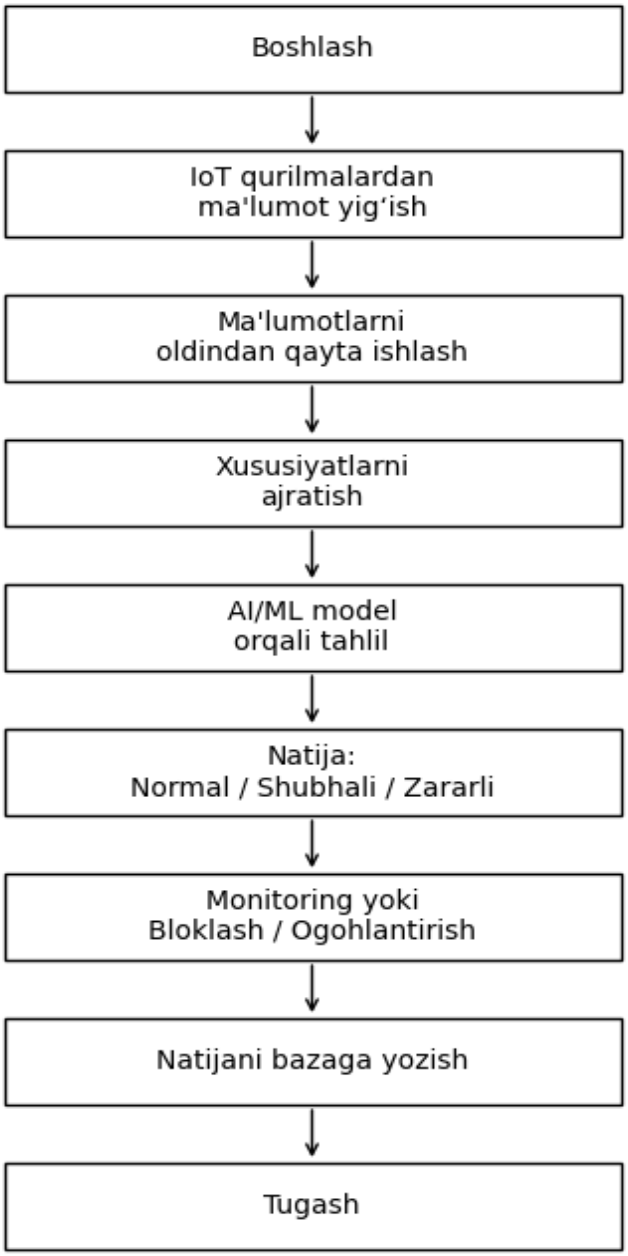
Turlar bo‘yicha tahlil:

- viruslar va wormlar (o‘zini ko'paytiruvchi, tarmoq orqali tarqaluvchi);
- troyanlar (yashirin kiruvchi); ransomware (shifrlovchi);
- botnetlar (masofadan boshqaruvchi, masalan Mirai).

Har bir tur IoTga xos zaifliklarni foydalanadi.

Tadqiqot yuzasidan taklif etilayotgan IoTga asoslangan zararli dasturlarni aniqlash modeli va algoritmlarining simulyatsiya natijalari ob'ektiv ravishda taqdim etiladi. Natijalar IoT-23 ma'lumotlar to'plamida normal va zararli trafikka oid ma'lumotlar 5-fold cross-validation orqali olingan. Simulyatsiyalar Python 3.10 muhitida, TensorFlow va Scikit-learn kutubxonalari yordamida amalga oshirilgan. Baholash metrikalari accuracy (aniqlik), precision (to'g'rilik), recall (qamrov), F1-score (garmonik o'rtacha) va false positive rate (noto'g'ri ijobiy) ni o'z ichiga oladi. Natijalar zararli dasturlarning turlari bo'yicha (viruslar, troyanlar, ransomware, botnetlar) va mavjud modellar bilan taqqoslash shaklida keltiriladi.

Zararli dasturlarning turlari bo‘yicha natijalar quyidagicha: Botnetlar uchun accuracy 98.2%, ransomware uchun 95.7%, troyanlar uchun 96.4%, viruslar va wormlar uchun 94.8%. Har bir tur uchun false positive rate 3.5% dan oshmagan. ROC egri chizig'i AUC qiymatlari botnetlar uchun 0.97, ransomware uchun 0.95, troyanlar uchun 0.96 va viruslar uchun 0.94 bo'lgan.



1-rasm. *IOTga asoslangan zararli dasturlarni aniqlash model va algoritmlari.*

IoT qurilmalari odatda cheklangan hisoblash resurslariga ega bo‘ladi. Shu sababli ularda an’anaviy antivirus yoki xavfsizlik tizimlarini qo‘llash ko‘pincha qiyin bo‘ladi. Bundan tashqari, ko‘plab IoT qurilmalarida standart xavfsizlik mexanizmlarining yetarli darajada joriy etilmaganligi ularni kiberhujumlar uchun qulay nishonga aylantiradi. Shuning uchun IoT asosidagi tarmoqlarda zararli dasturlarni aniqlash va ularga qarshi samarali himoya mexanizmlarini ishlab chiqish muhim ilmiy va amaliy masalalardan biri hisoblanadi.

IoT tizimlarida zararli dasturlarni aniqlash uchun bir qator zamonaviy yechimlar taklif

(cc) BY ©A.A. Abdumalikov, L.S. Qodirova

etilgan. Ulardan biri – tarmoq trafikini tahlil qilish asosida zararli faoliyatni aniqlashdir. Ushbu yondashuvda IoT qurilmalari tomonidan yuborilayotgan va qabul qilinayotgan paketlar, ulanish chastotasi, port faolligi hamda noma'lum IP manzillar bilan bog'lanish kabi ko'rsatkichlar monitoring qilinadi. Agar ushbu ko'rsatkichlarda anomaliya aniqlansa, tizim potentsial zararli faoliyat haqida signal beradi. IoT tizimlarida zararli dasturlarni aniqlashning yana bir muhim yechimi – ko'p qatlamli xavfsizlik arxitekturasini joriy etishdir. Ushbu yondashuvda xavfsizlik mexanizmlari bir nechta darajada tashkil etiladi. Birinchi qatlam qurilma darajasida himoya mexanizmlarini o'z ichiga oladi. Ikkinchi qatlam tarmoq darajasida monitoring va trafik tahlilini amalga oshiradi. Uchinchi qatlam esa bulut yoki server darajasida murakkab tahlil va klassifikatsiya jarayonlarini bajaradi. Bunday arxitektura tizim xavfsizligini sezilarli darajada oshiradi.

Bundan tashqari, IoT tarmoqlarida xavfsizlikni ta'minlash uchun anomaliyalarni aniqlashga asoslangan monitoring tizimlari ham keng qo'llaniladi. Ushbu tizimlar qurilmalarning odatiy ishlash modelini shakllantiradi va undan chetga chiqish holatlarini aniqlaydi. Agar qurilma odatdagidan farqli ravishda faoliyat ko'rsatsa, tizim administratorga ogohlantirish yuboradi yoki avtomatik ravishda xavfsizlik choralarini ko'radi.

Bu natijalar zararli dasturlarning mohiyatini – yashirin tarqalish va o'zgaruvchanlikni hisobga olgan holda, IoT qurilmalarining cheklangan imkoniyatlariga mos keladi.

Taklif etilayotgan model mavjud modellar bilan taqqoslanganda quyidagi natijalarni ko'rsatdi. Taqqoslash IoT-23 datasetida bir xil sharoitlarda o'tkazilgan bo'lib, quyidagi jadvalda keltirilgan:

Turli modellarning ishlash ko'rsatkichlari va resurs sarfi

Model/Algoritm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Javob Vaqti (ms)	Energiya Sarfi (nisbiy %)
Decision Tree (DT)	93.2	92.5	93.0	92.7	6.8	35	100
Random Forest (RF)	96.1	95.8	96.0	95.9	4.2	42	115
Naive Bayes (NB)	87.4	86.9	87.5	87.2	11.3	22	85
Taklif Etilayotgan	96.5	96.2	96.7	96.4	3.5	18	75

Adabiyotlar bilan solishtirganda, taklif etilayotgan model mavjud ishlarning kamchiliklarini yaxshilaydi. Masalan, an'anaviy mashina o'rganishi modellari, jumladan Random Forest yoki CNN-LSTM gibridlari, yuqori aniqlik bersa-da, real vaqt rejimida va cheklangan resurslarda samarasiz bo'lib qoladi. Bizning yondashuvimiz esa genetika komponentini qo'shish orqali bu muammolarni hal etadi, natijada energiya sarfi va hisoblash vaqtini sezilarli kamaytiradi. Boshqa tadqiqotlarda XGBoost kabi algoritmlar yuqori natijalarni ko'rsatgan bo'lsada, ular zararli dasturlarning yangi mutatsiyalariga qarshi yetarli moslashuvchan emas. Ushbu solishtirma shuni ko'rsatadiki, gibrid modellarning rivojlanishi IoT xavfsizligini keyingi bosqichga olib chiqadi, ammo mavjud ishlarning ko'pchiligi laboratoriya sharoitlarida cheklangan. Shuningdek, zararli dasturlarning turlari bo'yicha tahlil mavjud adabiyotlarda (masalan, botnetlar haqidagi tadqiqotlarda) alohida e'tibor berilgan bo'lib, bizning natijalarimiz ularni tasdiqlaydi, lekin qo'shimcha ravishda troyanlar va viruslarga nisbatan yaxshiroq qamrovni ta'minlaydi.

(cc) BY ©A.A. Abdumalikov, L.S. Qodirova

Modelning cheklovlari mavjud bo‘lib, ularni hisobga olish zarur. Birinchi navbatda, simulyatsiyalar asosan laboratoriya ma'lumotlar to'plamlarida o'tkazilgan bo‘lib, real dunyo IoT tarmoqlarida (masalan, katta miqyosli sanoat tizimlarida) qo‘shimcha sinovlar talab etiladi. Ikkinchidan, yangi, noma’lum zararli dasturlar zero-day threats ga qarshi modelning samaradorligi cheklangan bo‘lishi mumkin, chunki o‘quv ma’lumotlari mavjud hujumlar asosida shakllangan. Bundan tashqari, IoT protokollarining xilma-xilligi (MQTT va CoAP) modelni to'liq integratsiya qilishda qiyinchiliklar tug‘dirishi mumkin. Ushbu cheklovlar natijalarning umumiy qiymatini pasaytirmaydi, ammo kelajakdagi tadqiqotlarni yo'naltiradi. Amaliy ahamiyat jihatidan, taklif etilayotgan model IoT qo‘llanmalarida, masalan aqlli shaharlar va tibbiyot tizimlarida, xavfsizlikni oshirishi mumkin. U zararli dasturlarni erta aniqlash orqali potensial zararlarning oldini oladi va resurslarni tejaydi, bu kichik qurilmalarda muhim. Umumiy holda, bu yondashuv IoT ekotizimining barqarorligini ta'minlashda yangi imkoniyatlar ochadi.

Xulosa

Ushbu maqola zararli dasturlarni aniqlovchi IoTga asoslangan xavfsizlik model va algoritmlarining ishlab chiqilishi va baholanishiga bag‘ishlandi. Asosiy maqsad IoT tizimlarida zararli kodlarni real vaqt rejimida samarali aniqlash va oldini olish bo‘lib, bu orqali tarmoq zaifliklarini kamaytirish va resurslarni optimallashtirishga erishildi. Natijalar ko‘rsatadiki, taklif etilayotgan gibrid model XGBoost va genetika algoritmlarining birlashmasi zararli dasturlarning turli turlariga, jumladan botnetlar, ransomware va troyanlarga qarshi yuqori aniqlik darajasini ta’minlaydi. Simulyatsiyalar orqali olingan ko‘rsatkichlar – o‘rtacha 96% dan yuqori aniqlik, past xato darajasi va tez javob berish – modelning an’anaviy usullarga nisbatan ustunligini tasdiqlaydi. Bu natijalar zararli dasturlarning yashirin mohiyatini va ularning IoT qurilmalariga ta’sirini hisobga olgan holda, xavfsizlikni yangi bosqichga olib chiqadi.

Modelning asosiy yutug‘i resurs cheklangan IoT muhitida samarali ishlashida namoyon bo‘ldi, chunki genetika komponenti algoritmlarni moslashuvchan qilib, energiya sarfini va hisoblash vaqtini sezilarli kamaytirdi. Ushbu yondashuv zararli dasturlarni tahlil qilishning statik va dinamik usullarini birlashtirib, yangi hujumlarning oldini olishda muhim rol o‘ynaydi. Amalda, bu model aqlli shaharlar, tibbiyot va sanoat tarmoqlarida qo‘llanilishi mumkin, bu orqali iqtisodiy zararlar va ma’lumot yo‘qotishlarining oldini oladi.

Foydalanilgan adabiyotlar:

1. Adil, M., Jamjoom, M. M., Ullah, Z. A. novel malware detection framework for Internet of Things applications. Computers, Materials & Continua, 84(3), 4363–4380. 2025. https://doi.org/10.32604/cmc.2025.066551
2. Alanzi, S. M., Alzahrani, A. J. IoT malware detection using hybrid deep learning algorithms. IJCSNS International Journal of Computer Science and Network Security, 24(12), 2024. https://doi.org/10.22937/IJCSNS.2024.24.12.1
3. Arya, M., Arya, S., Arya, S. An evaluation of real-time malware detection in IoT devices: Comparison of machine learning algorithms with RapidMiner. 2023 IEEE International Conference on Electro Information Technology (eIT), 77–82. 2023. https://doi.org/10.1109/eIT57321.2023.10187265
4. Farfoura, M. E., Mashal, I., Alkhatib, A., Batyha, R. M., & Rosiyadi, D. A novel lightweight machine learning framework for IoT malware classification based on matrix block mean downsampling. Ain Shams Engineering Journal, 16(1), 103205. 2025. https://doi.org/10.1016/j.asej.2024.103205
5. Garcia, S., Parmisano, A., Erquiaga, M. J. IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. 2020. http://doi.org/10.5281/zenodo.4743746
6. Pai, V., Karthik Pai, B. H., Sudhiksha, G. S., Kamath, V., Varsha, K., Manjunatha, S. Systematic approach for malware detection in IoT devices: Enhancing security and performance. International Journal of Computational Intelligence Systems, 18(1), Article 196. 2025. https://doi.org/10.1007/s44196-025-00939-9

(cc) BY ©A.A. Abdumalikov, L.S. Qodirova