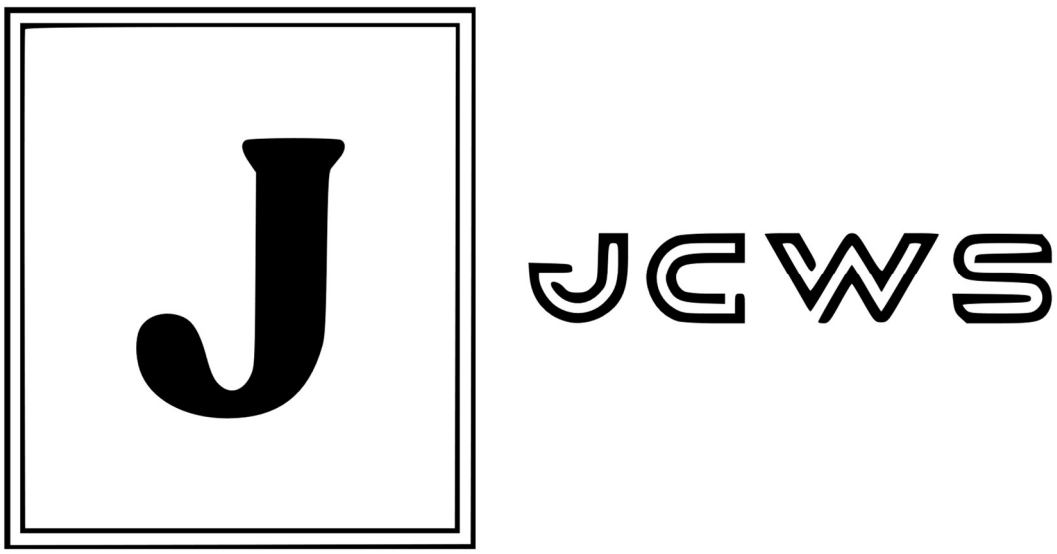
VOLUME | 4 ISSUE | 8 JANUARY 2026

JOURNAL OF CONTEMPORARY WORLD STUDIES

INDEX COPERNICUS INTERNATIONAL
OpenAIRE | EXPLORE
Google Scholar
ESEARCHBI IMPACT 2024 IF:10 FACTOR

INTERNATIONAL STANDARD SERIAL NUMBER UNITED STATES
Academic Resource Index ResearchBib
zenodo

VOLUME | 4 ISSUE | 8 |JANUARY |2026



ZARARLI DASTURLARNI ANIQLASHDA MASHINALI O‘QITISH TEXNOLOGIYALARINING ZAMONAVIY VOSITALARI

Abdumalikov Akmaljon Abduxoliq o‘g‘li [1]
Qodirova Laylo Sobir qizi [2]
Qarshibayeva O‘g‘iloy Abdunabi qizi [3]

Mirzo Ulug‘bek nomidagi O‘zMU Jizzax filiali dotsenti [1]
Mirzo Ulug‘bek nomidagi O‘zMU Jizzax filiali magistranti [2]
Mirzo Ulug‘bek nomidagi O‘zMU Jizzax filiali talabasi [3]
e-mail: akmalabdumalikov6@gmail.com, layloinomova9@gmail.com, qarshiboyevabdinabi@gmail.com

Accepted Date:
January 05, 2026,
Published Date:
January 15, 2026

Journal Website: https://d-pressa.com/index.php/jcws/

ANNOTATION:

Ushbu maqola zararli dasturlarni aniqlash mashinali o’qitish texnologiyalari va ularning zamonaviy vositalarining amaliy tadqiqi keltirilgan. Zararli dasturlarning mohiyati, turlari va IoTga ta’sirini tahlil qilib, mavjud aniqlash usullarining cheklovlari aniqlandi. Taklif etilgan model hamda tizimli arxitektura mashinali o’qitishning zamonaviy algoritmlari 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.

KEYWORDS:

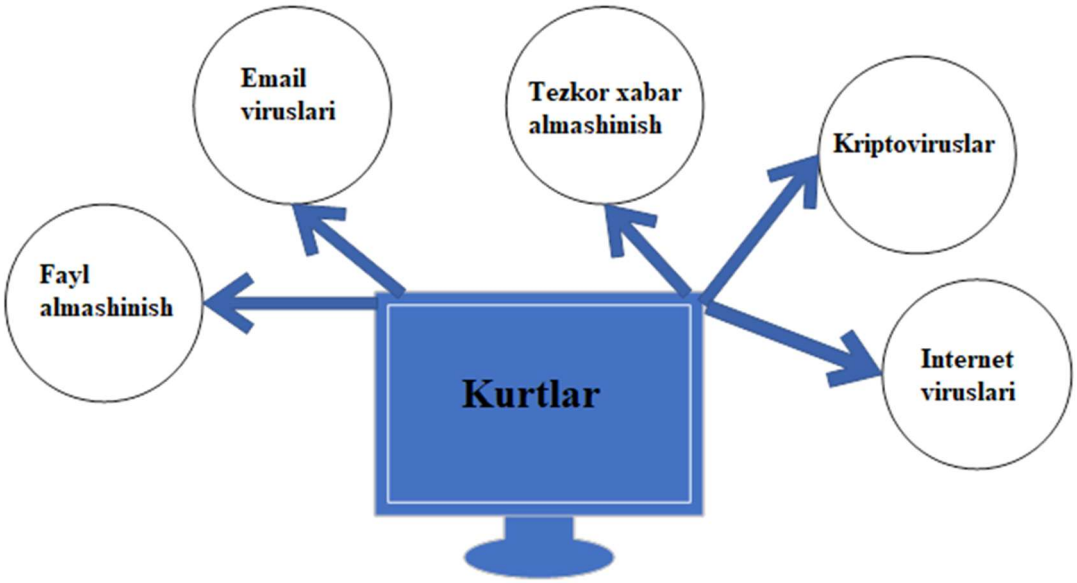
IoT xavfsizligi, zararli dasturlar, malware aniqlash, XGBoost, genetika algoritmi, gibrid model.

Kirish

Kompyuter qurtlari (worms) – bu zararli dasturiy ta’minotning o‘z-o‘zini tarqatish va mustaqil ravishda ko‘payish xususiyatiga ega bo‘lgan shaklidir. Ular viruslardan farqli o‘laroq, mezbon faylga ulanmasdan, to‘g‘ridan-to‘g‘ri tarmoq orqali tarqaladi. Qurtlar yaratilishi va rivojlanishi quyidagi bo‘lgan, Qurt yaratuvchilari dastlab tarmoqdagi ko‘plab tizimlarga avtomatik kirish, zaifliklarni ekspluatatsiya qilish yoki zararli payload (masalan, ma’lumotlarni o‘g‘irlash, tizimga masofadan kirish imkoniyati yaratish) bajarish kabi maqsadlar asosida g‘oyani shakllantiradilar. Dastlabki maqsad – tarmoq resurslarida yuz berayotgan zaifliklardan foydalanib, qurtni tez va keng tarqatish. Bu orqali u o‘zining nusxalarini ko‘paytiradi va har bir topilgan zaif tizimga kirib, o‘zini joylashtiradi. Qurtlar odatda tizim yaqin tillarda yoki ba’zan skript tillarida yoziladi. Bu tillar yordamida yozilgan kod operator tizim resurslariga, tarmoq protokollariga va xavfsizlik chambarchasligi zaif joylariga kirish imkoniyatini beradi. Yaratuvchi dasturchi qurt kodini shunday loyihalashtiradiki, u:

- tarmoqdagi ochiq portlar va zaifliklarni avtomatik skaner qiladi;
- topilgan zaif tizimlarga o‘zini replikatsiya qiladi;
- zarur bo‘lsa, o‘z kodini polimorfik usullar orqali o‘zgartiradi, bu esa antivirüs tizimlari tomonidan aniqlanishni qiyinlashtiradi;

-



1-rasm. Kompyuter qurtlarining turlari.

Asosiy qism

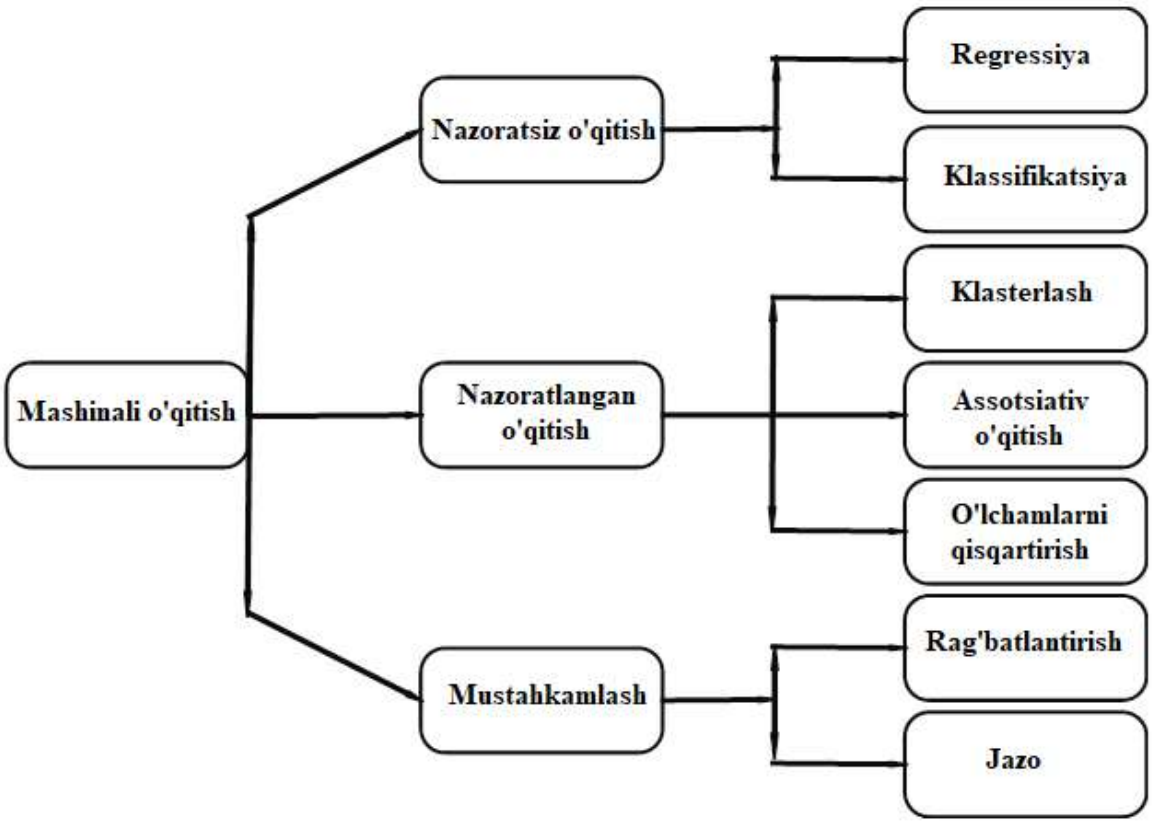
Qurt yaratilishida asosiy e’tibor tarmoqdagi bog‘lanishlarni va ochiq portlarni aniqlashga qaratilgan. Dastur doimiy ravishda IP manzillar oralig‘ida skanerlash olib boradi va zaif tizimlarni izlaydi. Zaif tizim topilgach, qurt o‘zining nusxasini shu tizimga yuboradi va shu orqali tarmoq bo‘ylab o‘z-o‘zini tarqatadi. Bu jarayon, masal uchun, Morris Worm kabi dasturlar orqali realizatsiya qilingan; u tarmoqdagi zaifliklar orqali tezda ko‘plab kompyuterlarga kirib, o‘zini nusxalashni amalga oshirgan. Yaratilgan qurt dasturi maxsus test muhitlarida (sandbox) sinovdan o‘tkaziladi. Bu bosqichda uning tarqalish tezligi, zaifliklardan foydalanish samaradorligi va potensial zararli payloadning ish faoliyati aniqlanadi. Sinovlar natijasida aniqlangan xatoliklar va

antivirus tizimlari orqali aniqlanish ehtimoli kamaytiriladi. Shu tariqa, kodda kerakli o‘zgarishlar kiritib, qurtning ishlash samaradorligini oshirishga erishiladi. Qurtlar odatda elektron pochta, veb-skanerlar, tarmoq protokollari yoki boshqa ko‘plab kanallar orqali tarqatiladi. Maqsad – minimal inson aralashuvida, avtomatik va keng tarqalish. Antivirus va xavfsizlik tizimlari qurtlarni aniqlashga harakat qilayotganligi sababli, yaratuvchilar o‘z kodlarini shifrlash yoki obfuskatsiya (murakkablashtirish) usullaridan foydalanadilar. Bu qurtning aniqlanish ehtimolini sezilarli darajada kamaytiradi. Qurtlar yaratilishi kiberxavfsizlik sohasidagi innovatsion va tajriba asosidagi yondashuvlarning natijasi bo‘lib, ular tarmoqdagi zaifliklardan maksimal darajada foydalanishga qaratilgan. Dasturchilar o‘z kodlari yordamida avtomatik ravishda tizimlarni skanerlash, ular orasida zaifliklarni aniqlash, va o‘zini tarqatish mexanizmlarini ishlab chiqadilar. Ushbu jarayon kiberhujumlarga qarshi himoya tizimlarini doimiy ravishda takomillashtirish va yangi antivirus strategiyalarini ishlab chiqish uchun qimmatli tajriba va darslar beradi.

Josus dasturlar (Spyware) – bu foydalanuvchining ruxsatisiz ma’lumotlarni yig‘ish va ularni uchinchi tomonlarga yetkazish uchun mo‘ljallangan zararli dasturiy ta’minotdir. Josus dasturlar odatda maxfiy ma’lumotlarni yig‘ish (masalan, login, parol, bank ma’lumotlari), foydalanuvchi faoliyatini kuzatish yoki reklama maqsadida ishlatiladi. Yaratuvchi dasturdan qanday maqsadda foydalanishni belgilaydi. Spyware dasturlari ko‘pincha C++, Python yoki Java kabi tillarda yoziladi. Bu tillar tizim resurslariga kirish va ma’lumotlarni yig‘ish imkoniyatini beradi. Josus dastur foydalanuvchining faoliyatini kuzatish uchun tizim API-laridan foydalanadi. Masalan, klaviatura bosishlarini qayd etish, ekran tasvirlarini olish yoki tarmoq faoliyatini kuzatish kabi funksiyalarni amalga oshiradi. Josus dasturlar antivirus dasturlar tomonidan aniqlanishni qiyinlashtirish uchun obfuskatsiya (kodni murakkablashtirish) va shifrlash usullaridan foydalanadi. Josus dasturlar zararli elektron pochta, soxta dasturlar yoki phishing havolalari orqali tarqatiladi. Ba’zan ular rasmiy dastur do‘konlari orqali ham tarqalishi mumkin.

Mashinali o‘qitish - sun’iy intellektning muhim yo‘nalishlaridan biri bo‘lib, u kompyuter tizimlariga inson yordamisiz ma’lumotlardan o‘rganish va mustaqil qarorlar qabul qilish imkonini beradi. Ushbu texnologiya ma’lumotlarni tahlil qilish va ulardan naqshlarni aniqlash orqali bashoratlar qilishga asoslanadi. Mashinali o‘qitish algoritmlari kompyuter dasturlarini o‘zgartirish yoki qayta dasturlashga ehtiyoj sezmasdan muayyan vazifalarni bajarishga qodir.

Bugungi raqamli davrda mashinali o‘qitish hayotning deyarli barcha sohalariga kirib bormoqda va inson faoliyatining samaradorligini oshirishda kata ahamiyatga ega. Har bir sohada foydalanish darajasiga qarab o‘ziga xos xususiyatga va afzalliklarga ega hisoblanadi. Masalan: sog‘liqni saqlashda;tibbiy ko‘rik natijalarini tahlil qilish, kasalliklarni oldindan aniqlash maq sadida, moliyaviy texnologiyalarda; Firibgarlikni aniqlash; kredit xavfini baholash uchun, avtonom tizimlarda-robotlar, dronlar va avtonom transport vositalarining boshqaruvini engillashtirish maqsadida, kundalik hayotda-tavsiya tizimlari (Netflix, Amazon), ovozli yordamchilar (Siri, Alexa). Ushbu texnologiya ma’lumot hajmining eksponensial o‘sishi va hisoblash quvvatining oshishi tufayli yanada muhim ahamiyat kasb etmoqda.



2-rasm. Zararli dasturlani aniqlashda mashinali o‘qitishning tarkibi.

Xulosa

Zararli dasturlar sonining ortib borishi va fayl murakkablashuvi an'anaviy himoya qilishmoqda. Shu sababli zararli dasturlarni ishlab chiqarishda mashinali o'quv texnologiyalaridan keyingi zamonaviy kiberxavfsizlik tizimlarining muhim yo'nalishiga aylanmoqda. Dasturiy ta'minot manbalari shuni ko'rsatadiki, mashinani o'rnatish algoritmlari katta hajmdagi ma'lumotlarni tahlil qilish orqali zararli dastur.

Maqolada ko'rib chiqish algoritmlari statik va dinamik tahlillarning usullarini qo'llash usullari, klassifikatsiyalash algoritmlari hamda chuqur o'rganish modeli qo' dasturiy dasturlarni aniqligini yanada chuqurlashtirishga asoslab berildi. barcha, sun'iy neyron tarmoqlari va chuqur o'qitish model qo'llarining murakkab va yashirin yuk-ni tekshirishni boshqarishadi. Shu bilan birga, shu bilan birga, dasturiy ta'minot asosidagi tizimlarni egallashda katta hajmdagi sifatli ma'lumotlar bazasining zarurligi, mashinaga yuklangan mahsulotlarga va noto'g'ri ta'sirga ega bo'lgan talab pozitiv mahsulotlarga tegishli muammolar ham aniqlandi. Umuman olganda, mashinali o'qitish texnologiyalari zararli dasturlarni aniqlashda, yuqori aniqlik, avtomatik ravishda va avtomatik ravishda aniqlashda muhim kasb etadi. Kelgusida intellekt asosidagi adaptiv va o'zo'zini rivojlantiruvchi sun'iy yo'llarga qarshi mahsulotlarni ishlab chiqarish dasturiy dasturlari kurashning eng istiqbolli narsalaridan biri hisoblanadi.

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