ISNN 3030-3907

2026/4
VOLUME 8

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/4 VOLUME 8

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

PE FAYLLARNING STATIK XUSUSIYATLARI ASOSIDA ZARARLI DASTURLARNI MODULLI ANSAMBL YORDAMIDA ANIQLASH

Turdimatov Mamirjon Mirzayevich
Farg‘ona davlat texnika universiteti
Olimov Fayozbek Fazliddin o‘g‘li
Farg‘ona davlat texnika universiteti

Annotatsiya. Maqolada Windows oilasiga mansub Portable Executable (PE) fayllarning statik xususiyatlari asosida zararli dasturlarni aniqlashga qaratilgan modulli ansambl yondashuvi ko‘rib chiqiladi. Tadqiqotda PE/header maydonlari, sectionlar statistikasi va entropiya, import va eksportga oid belgilar EMBER (v2) ma’lumotlar to‘plamidagi 2381 o‘lchamli xususiyatlar asosida uch mantiqiy blokka ajratildi. Birinchi blok uchun Random Forest, ikkinchi blok uchun XGBoost, uchinchi blok uchun esa LightGBM modeli tanlandi. Tajriba natijalari vaznli ansamblning 0.9567 F1-score va 0.9893 ROC-AUC, stacked ansamblning 0.9585 F1-score va 0.9915 ROC-AUC ko‘rsatkichlariga erishganini ko‘rsatdi. Olingan natijalar PE fayllarning strukturaviy va statistik xususiyatlarini alohida modullarda qayta ishlash hamda ularni ansambl darajasida birlashtirish statik aniqlashning aniqligi va barqarorligini oshirishini tasdiqlaydi.

Kalit so‘zlar. Zararli dastur, statik tahlil, PE fayl, EMBER, Random Forest, XGBoost, LightGBM, ansambl klassifikatsiya, entropiya

Abstract. The paper presents a modular ensemble approach to detect malware based on static features of Windows Portable Executable (PE) files. In the study, PE/header fields, section statistics, and entropy, import and export symbols were divided into three logical blocks based on 2381 dimensional features in the EMBER (v2) dataset. Random Forest was selected for the first block, XGBoost for the second block, and LightGBM for the third block. Experimental results showed that the weighted ensemble achieved 0.9567 F1-score and 0.9893 ROC-AUC, and the stacked ensemble achieved 0.9585 F1-score and 0.9915 ROC-AUC. The obtained results confirm that processing the structural and statistical features of PE files in separate modules and combining them at the ensemble level increases the accuracy and stability of static detection.

Keywords. Malware detection, static analysis, Portable Executable, EMBER, Random Forest, XGBoost, LightGBM, ensemble learning, entropy

Аннотация. В статье представлен модульный ансамблевый подход к обнаружению вредоносных программ на основе статических характеристик исполняемых файлов Windows (PE). В исследовании поля заголовка PE-файлов, статистика разделов, энтропия, символы импорта и экспорта были разделены на три логических блока на основе 2381-мерных характеристик из

ISSN 3030-3907

набора данных EMBER (v2). Для первого блока был выбран алгоритм Random Forest, для второго — XGBoost, а для третьего — LightGBM. Экспериментальные результаты показали, что взвешенный ансамбль достиг показателя F1-меры 0,9567 и ROC-AUC 0,9893, а стековый ансамбль — показателя F1-меры 0,9585 и ROC-AUC 0,9915. Полученные результаты подтверждают, что обработка структурных и статистических характеристик PE-файлов в отдельных модулях и их объединение на уровне ансамбля повышает точность и стабильность статического обнаружения.

Ключевые слова. Обнаружение вредоносных программ, статический анализ, портативные исполняемые файлы, EMBER, Случайный лес, XGBoost, LightGBM, ансамблевое обучение, энтропия

KIRISH.

Zararli dasturlarni aniqlash bo‘yicha an’anaviy signaturaga asoslangan yondashuvlar ma’lum namunalarni tez topa olsa-da, polimorfizm, packing va nol-kun (zero-day) tahdidlari sharoitida ularning moslashuvchanligi cheklangan. Shu sababli so‘nggi yillarda PE fayllarning statik xususiyatlariga tayangan mashinaviy o‘qitish usullari alohida ahamiyatga ega [1], [2]. Statik tahlilning afzalligi shundaki, faylni ishga tushirmasdan turib, uning strukturasi, sectionlari va import jadvali asosida xavf profili shakllantiriladi. Bunday yondashuv katta hajmli obyektlarni oldindan skrining qilish uchun qulaydir.

Windows muhitidagi bajariluvchi obyektlar Portable Executable formatida saqlanadi. Microsoft spetsifikatsiyasiga ko‘ra, PE tuzilmasi DOS header, COFF header, optional header, data directory va section jadvalidan iborat bo‘lib, aynan shu qatlamlar statik tahlil uchun boy belgilar manbaini hosil qiladi [1]. Header maydonlari dastur yuklanish sxemasini, sectionlar statistikasi packed yoki siqilgan tarkib belgilarini, import va eksportlar esa funksional niyatni bilvosita aks ettiradi.

Maqolaning maqsadi PE fayllarning strukturaviy, statistik va semantik belgilarini alohida modullarda qayta ishlovchi ansambl yondashuvining samaradorligini ko‘rsatishdir. Tajribada Random Forest, XGBoost va LightGBM modullari tanlanib, ularning chiqishlari vaznli ansambl va stacked meta-klassifikator orqali birlashtirildi. Tadqiqot natijalari haqiqiy o‘qitish va testlash natijalari asosida taqdim etiladi.

ADABIYOTLAR TAHLILI

PE fayllarga asoslangan zararli dasturlar tahlili bo‘yicha ochiq benchmarklardan eng ko‘p qo‘llaniladiganlaridan biri EMBER to‘plamidir. Anderson va Roth tomonidan taklif etilgan ushbu to‘plam 1.1 million PE fayldan ajratilgan xususiyatlarni o‘z ichiga oladi hamda PE header, section entropiyalari, importlar va satr statistikasi kabi belgilarni standartlashtirilgan ko‘rinishda beradi

ISSN 3030-3907

[2]. EMBER nafaqat modellarni qiyoslash, balki amaliy avtomatlashtirilgan bosqichlar ketma-ketligini qayta ishlab chiqish uchun ham qulay asos hisoblanadi.

PE formatining o‘zi tadqiqot uchun muhim nazariy poydevor yaratadi. Microsoft hujjatlarida PE strukturasining headerlar, ma’lumot kataloglari va sectionlar qatlamiga ajralishi ko‘rsatilgan bo‘lib, bu qatlamlar malware va benign namunalarning strukturaviy farqlarini ushlash imkonini beradi [1]. So‘nggi tadqiqotlarda ham header maydonlari, entropiya, import jadvali va eksportlar statik aniqlashning asosiy belgilar manbai sifatida ko‘rsatilmoqda [6], [7].

Model tanlovi bo‘yicha adabiyotlarda daraxtsimon ansambl algoritmlari ustunlik qilmoqda. Random Forest heterogen va masshtablari turlicha bo‘lgan PE/header belgilarini qayta ishlashda barqarorligi bilan ajralib turadi [3]. XGBoost esa gradient boosting asosida nolinear bog‘liqliklarni chuqurroq aniqlaydi va katta hajmli tabulyar ma’lumotlar uchun samarali hisoblanadi [4]. LightGBM esa GOSS va EFB mexanizmlari hisobiga katta va siyrak xususiyatlar to‘plamida tezkor o‘qitish imkonini beradi [5]. 2025-yildagi tadqiqotlarda ham aynan LightGBM va XGBoost EMBER asosidagi zararli dasturlarni aniqlash vazifalarida eng barqaror natijalarni bergani qayd etilgan [7], [8].

Adabiyotlarni umumlashtirib aytganda, statik aniqlashda bitta modeldan ko‘ra turli belgilar bloklari uchun mos modellarni tanlash va ularni ansambl darajasida birlashtirish istiqbolli yo‘nalish sifatida namoyon bo‘lmoqda. Shunga qaramay, ko‘plab ishlarda PE/header, statistika va import semantikasi bir xil modelda ko‘riladi. Ushbu tadqiqotda esa ushbu uch qatlam alohida modullarga ajratilib, ularning ansambl kombinatsiyasi real tajriba natijalari bilan baholandi.

TADQIQOT METODOLOGIYASI.

Tadqiqot uchun EMBER v2 vektorlashtirilgan ma’lumotlari tanlandi. O‘qitish jarayonida yorlig‘i mavjud namunalar ajratilib, 480 000 ta namuna trening, 120 000 ta namuna validatsiya va 200 000 ta namuna test qismiga ajratildi. EMBER vektorining 2381 o‘lchami uch semantik blokka bo‘lindi: birinchi blokka general PE metadata, header va data directory maydonlari; ikkinchi blokka byte histogram, byte-entropy histogram, string statistics va section statistics; uchinchi blokka esa import va eksportga oid xususiyatlar kiritildi. Bunday taqsimot PE faylning strukturaviy, statistik va funksional qatlamlarini alohida ko‘rishga imkon berdi.

Statistik blok uchun Shannon entropiyasi muhim ko‘rsatkichlardan biridir. Agar p_i (i=0…255) i-bayt qiymatining nisbiy ulushini bildirsa, entropiya quyidagicha hisoblanadi:

ISSN 3030-3907

$$H(x) = -\sum_{i=0}^{255} p_i log_2(p_i)$$

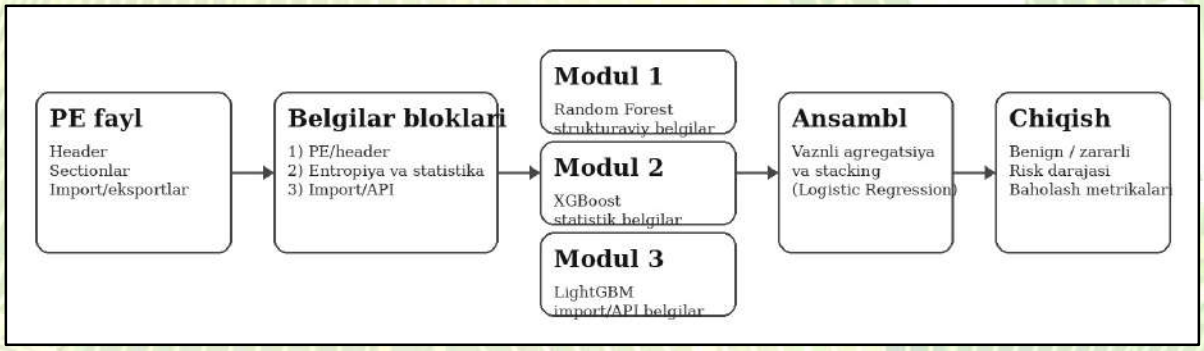
PE/header blokida Random Forest tanlanishining sababi uning strukturaviy va bayroq tipidagi xususiyatlar bilan yaxshi ishlashi, oldindan masshtablashga yuqori darajada bog‘liq emasligi va xususiyatlar o‘rtasidagi nolinear o‘zaro ta’sirlarni ushlay olishidir [3]. Entropiya va section statistikasi uchun XGBoost tanlandi, chunki ushbu blokdagi belgilar ko‘pincha murakkab kombinatsion bog‘liqliklar hosil qiladi; XGBoost esa hist usuli va boosting mexanizmi orqali bunday vazifalarda yuqori aniqlik beradi [4]. Import va eksportga oid belgilar uchun LightGBM tanlandi, chunki ushbu fazo nisbatan siyrak va katta o‘lchamli bo‘lib, LightGBM katta ma’lumotlarda o‘qitish tezligi bilan ajralib turadi [5], [8].

Bazaviy modullar ehtimollari dastlab vaznli ansambl orqali birlashtirildi. Vaznlar validatsiya to‘plamidagi F1-score qiymatlariga mutanosib ravishda tanlandi. Ansambl ehtimoli quyidagi ifoda bilan hisoblandi:

$$P = w_1 p_{RF} + w_2 p_{XGB} + w_3 p_{LGBM}$$

Bu yerda p_{RF}, p_{XGB}, p_{LGBM} - mos ravishda header, statistik, import/API modullarining ehtimollari, w_1, w_2, w_3 - esa ularning vaznlari bo‘lib $w_1 + w_2 + w_3 = 1$.

Validatsiya natijalari asosida $w_1 = 0.3457, w_2 = 0.3381, w_3 = 0.3162$ qiymatlari hosil qilindi. Bundan tashqari, uch modul chiqishlari ustida Logistic Regression meta-klassifikatori yordamida stacked ansambl ham qurildi. Baholash uchun accuracy, precision, recall, F1-score va ROC-AUC metrikalari qo‘llanildi.



1-rasm. PE fayllarning statik tahliliga asoslangan modulli ansambl sxemasi

MUHOKAMA VA NATIJALAR.

Test to‘plamidagi natijalar bazaviy modullar va ansambl yondashuvining sezilarli farqini ko‘rsatdi. Random Forest PE/header moduli 0.94557 accuracy va 0.94492 F1-scorega, XGBoost statistik moduli 0.92276 accuracy va 0.92457 F1-scorega, LightGBM import moduli esa 0.85505 accuracy va 0.85538 F1-scorega erishdi. Import modulining yakka holdagi aniqligi pastroq bo‘lsa-da, uning semantik signali ansamblga qo‘shimcha diversifikatsiya olib kirdi. Natijada vaznli

ISSN 3030-3907

ansambl 0.95673 accuracy va 0.95674 F1-score, stacked ansambl esa 0.95846 accuracy va 0.95851 F1-score ko‘rsatdi.

1-jadval.

Test to‘plamidagi bazaviy modullar va ansambl natijalari

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Random Forest (PE/header)	0.94557	0.95642	0.93368	0.94492	0.98785
XGBoost (statistika)	0.92276	0.90339	0.94677	0.92457	0.97905
LightGBM (import/eksport)	0.85505	0.85346	0.85730	0.85538	0.93194
Vaznli ansambl	0.95673	0.95646	0.95701	0.95674	0.98930
Stacked ansambl	0.95846	0.95736	0.95966	0.95851	0.99151

Hisoblash samaradorligi ham alohida e’tiborga loyiq. Trening loglariga ko‘ra, Random Forest moduli 1 daqiqa 21.7 soniyada, XGBoost moduli 2 daqiqa 17.2 soniyada, LightGBM moduli esa 35.38 soniyada o‘qitildi. Logistic Regression asosidagi stacked meta-klassifikator 0.32 soniyada tayyorlandi. Modelni yuklash, baholash va saqlash bilan birga umumiy vaqti 6 daqiqa 9.7 soniyani tashkil etdi. Bu natijalar LightGBM’ning import/eksport blokida tanlanishi nafaqat aniqlik, balki hisoblash tejamkorligi nuqtai nazaridan ham asosli ekanini ko‘rsatadi [5].

2-jadval.

Modellarni o‘qitishning amaliy vaqt sarfi

Bosqich	Vaqt
EMBER ni yuklash	1m 1.8s
Random Forest	1 min 21.7 s
XGBoost	2 min 17.2 s
LightGBM	35.38 s
Stacked meta-model	0.32 s
To‘liq o‘qitish/baholash/saqlash	6 min 9.7 s

Natijalar tahlili shuni ko‘rsatadiki, PE/header moduli strukturaviy anomaliyalarni yaxshi tutadi, statistik modul packed va obfuskatsiyalangan namunalarga nisbatan sezgirroq, LightGBM moduli esa import va eksportlar semantikasidan foydalanib ansamblning umumlashtirish qobiliyatini oshiradi. Yakka modul sifatida eng yuqori accuracy Random Forestda kuzatilgan bo‘lsa-da,

ISSN 3030-3907

ROC-AUC bo‘yicha stacked ansambl 0.99151 natija bilan eng yuqori ko‘rsatkichni berdi. Demak, belgilarni semantik bloklarga ajratish va ularni ansambl darajasida birlashtirish PE fayllar asosidagi statik aniqlashda amaliy jihatdan o‘zini oqlaydi.

XULOSA.

PE fayllarning strukturaviy, statistik va importga oid belgilarini alohida modullarda qayta ishlashga asoslangan yondashuv statik malware detection vazifasi uchun samarali ekani tajribada tasdiqlandi. Random Forest PE/header qatlamidagi murakkab strukturaviy bog‘liqliklarni, XGBoost entropiya va section statistikalarini, LightGBM esa import/eksport semantikasini qayta ishlashda mos tanlov bo‘ldi. Tadqiqot shuni ko‘rsatadiki, PE faylning turli qatlamlarini bitta yagona modelga emas, balki belgilar tabiatiga mos algoritmlarga taqsimlash aniqlikni oshiradi va modelning barqarorligini kuchaytiradi. Shu bilan birga, LightGBM modulining qisqa o‘qitish vaqti katta hajmli ma’lumotlarda hisoblash samaradorligi nuqtai nazaridan muhim afzallik berdi. Keyingi izlanishlarda xususiyatlarni vaqt bo‘yicha driftga mos qayta kalibrlash, packing ta’sirini alohida baholash va meta-ansamblning yanada moslashuvchan variantlarini sinash maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR

1. Microsoft, “PE Format - Win32 apps,” Microsoft Learn, Jul. 14, 2025. [Online]. Manba: https://learn.microsoft.com/en-us/windows/win32/debug/pe-format

2. H. S. Anderson and P. Roth, “EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models,” arXiv:1804.04637, 2018. [Online]. Manba: https://arxiv.org/abs/1804.04637

3. L. Breiman, “Random Forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001. [Online]. Manba: https://link.springer.com/article/10.1023/A:1010933404324

4. T. Chen and C. Guestrin, “XGBoost: A Scalable Tree Boosting System,” in Proc. 22nd ACM SIGKDD, 2016, pp. 785–794. [Online]. Manba: https://doi.org/10.1145/2939672.2939785

5. G. Ke et al., “LightGBM: A Highly Efficient Gradient Boosting Decision Tree,” in Advances in Neural Information Processing Systems 30, 2017. [Online]. Manba: https://proceedings.neurips.cc/paper/2017/hash/6449f44a102fde848669bdd9eb6b76fa-Abstract.html

6. M. I. Yousuf, M. A. A. Babar, and H. J. Al-Dulaimi, “Windows malware detection based on static analysis with machine learning methods,” PeerJ Computer Science, vol. 9, e1319, 2023. [Online]. Manba: https://peerj.com/articles/cs-1319/

ISSN 3030-3907

7. M. M.-H.-Z. Abedin and T. Mehrub, “Evaluating Ensemble and Deep Learning Models for Static Malware Detection with Dimensionality Reduction Using the EMBER Dataset,” arXiv:2507.16952, 2025. [Online]. Manba: https://arxiv.org/abs/2507.16952

8. A. Verma, “An Optimized LightGBM Framework for Static Malware Detection,” Int. J. Comput. Sci. Machine Analytics, 2025. [Online]. Manba: https://submissions.adroidjournals.com/index.php/ijcma/article/view/208

9. D. Gibert, C. Mateu, and J. Planes, “Assessing the impact of packing on static machine learning-based malware detection and classification systems,” Computers & Security, vol. 149, 104110, 2025. [Online]. Manba: https://doi.org/10.1016/j.cose.2025.104110

ISSN 3030-3907