

MESSENERLARDA TARQALADIGAN PHISHING, MALWARE VA SCAM TAHDIDLARINI REAL VAQT REJIMIDA ANIQLASH VA TAHLIL QILISH TIZIMLARI

Eshchanov Shamsiddin Zaripboy o'g'li
"Toshkent amaliy fanlar universiteti", talabasi
eshchanovsh04@gmail.com +998(94)-404-34-56

Annotatsiya: Ushbu maqolada messenjer ilovalarida tarqaladigan fishing, zararli dasturlar (malware) va firibgarlik (scam) tahdidlarini real vaqt rejimida aniqlash va tahlil qilish tizimlarini ishlab chiqishning metodologik va amaliy jihatlarini ko'rib chiqadi. Tadqiqotda sun'iy intellekt va mashina o'qitish (AI/ML) usullari, tabiiy tilni qayta ishlash (NLP) algoritmlari, xatti-harakatlar tahlili va kriptografik imzolarni tekshirish texnologiyalari integratsiyalashgan arxitektura taklif qilinadi. Natijalar shuni ko'rsatadiki, taklif etilayotgan tizim 94,2% aniqlik bilan tahdidlarni aniqlashga qodir bo'lib, real vaqt rejimida 50 ms dan kam kechikish bilan ishlaydi. Ushbu natijalar messenjer xavfsizligini oshirish va foydalanuvchi ma'lumotlarini himoya qilishda muhim ahamiyatga ega.

Kalit so'zlar: Messenjer xavfsizligi, real vaqt rejimida aniqlash, fishing, zararli dastur, firibgarlik, sun'iy intellekt, mashina o'qitish, NLP, xavfsizlik tahlili.

Аннотация: В данной статье рассматриваются методологические и практические аспекты разработки систем обнаружения и анализа фишинговых, вредоносных программ (malware) и мошеннических (scam) угроз, распространяемых в мессенджерах, в режиме реального времени. В исследовании предлагается архитектура, интегрирующая методы искусственного интеллекта и машинного обучения (ИИ/МО), алгоритмы обработки естественного языка (NLP), анализ поведенческих паттернов и технологии проверки криптографических подписей. Результаты демонстрируют, что предлагаемая система способна выявлять угрозы с точностью 94,2%, работая в режиме реального времени с задержкой менее 50 мс. Данные результаты имеют важное значение для повышения безопасности мессенджеров и защиты пользовательских данных.

Ключевые слова: Безопасность мессенджеров, обнаружение в реальном времени, фишинг, вредоносное ПО, мошенничество, искусственный интеллект, машинное обучение, обработка естественного языка, анализ угроз.

Abstract: This article examines the methodological and practical aspects of developing real-time detection and analysis systems for phishing, malware, and scam threats distributed via messenger applications. The study proposes an integrated architecture combining artificial intelligence and machine learning (AI/ML) techniques, natural language processing (NLP) algorithms, behavioral pattern analysis, and cryptographic signature verification technologies. Results indicate that the proposed system achieves a detection accuracy of 94.2%, operating in real-time with a latency of less than 50 ms. These findings hold significant importance for enhancing messenger security and protecting user data.

Keywords: messenger security, real-time detection, phishing, malware, scam, artificial intelligence, machine learning, NLP, threat analysis.

KIRISH

Hozirgi kunda raqamli xavfsizlik masalalari axborot texnologiyalari rivojining ajralmas qismiga aylangan. Ijtimoiy tarmoqlar va messenjerlar, xususan Telegram, foydalanuvchilar

oʻrtasida eng ommabop aloqa vositalaridan biri sifatida keng qoʻllanmoqda. Shu bilan birga, bu muhitda kiberjinoyatchilar tomonidan foydalanuvchilarning ishonchidan foydalanib, phishing (soxta havolalar orqali maʼlumot oʻgʻirlash) hujumlarini amalga oshirish holatlari ham koʻpaymoqda. Phishing havolalar koʻpincha rasmiy koʻrinishga ega boʻlib, foydalanuvchini firibgarlik sahifalariga yoʻnaltiradi va natijada foydalanuvchi parol, login yoki moliyaviy maʼlumotlarini yoʻqotadi. Shu sababli, Telegram muhitida real vaqt rejimida phishing havolalarni aniqlash va foydalanuvchini himoya qilish muhim masalalardan biridir.

Soʻnggi oʻn yillikda messenger ilovalari (Telegram, WhatsApp, Signal, Viber va boshqalar) shaxsiy, ijtimoiy va korporativ muloqotning asosiy vositasiga aylandi. Shu bilan birga, ular kiberjinoyatchilar uchun qulay nishonga aylangan boʻlib, fishing havolalari, zararli dasturlar (malware) va ijtimoiy muhandislikka asoslangan firibgarlik (scam) hujumlari tez surʼatlar bilan oʻsib bormoqda. Messengerlarning end-to-end shifrlash (E2EE) arxitekturasini xabarlarining maxfiyligini taʼminlasada, tahdidlarni real vaqt rejimida tahlil qilishni qiyinlashtiradi. Anʼanaviy antivirus va qoidaga asoslangan (rule-based) himoya tizimlari yangi, nomaʼlum tahdidlarga nisbatan zaif boʻlib, ular koʻpincha post-factum tahlilga tayanadi.

Ushbu tadqiqotning maqsadi messengerlarda tarqaladigan phishing, malware va scam tahdidlarini real vaqt rejimida aniqlash va tahlil qilish uchun koʻp qatlamli, sunʼiy intellektga asoslangan tizim arxitekturasini ishlab chiqish va uning samaradorligini baholashdir. Tadqiqot quyidagi masalalarni yoritadi:

1. shifrlangan muhitda tahdidlarni qanday qilib metamaʼlumotlar va xatti-harakatlar tahlili orqali aniqlash mumkin;
2. real vaqt rejimida ishlash uchun qaysi AI/ML va stream processing texnologiyalari optimal;
3. taklif etilayotgan yechimning amaliy joriy etish imkoniyatlari va cheklovlari qanday.

Messengerlarda (Telegram, WhatsApp, Signal) tarqaladigan phishing, malware (zararli dasturlar) va scam (firibgarlik) tahdidlarini real vaqt rejimida aniqlash — bu sunʼiy intellekt (AI), mashinali oʻqitish (ML) va tabiiy tilni qayta ishlash (NLP) texnologiyalariga asoslangan murakkab tizimdir. Ushbu tizimlar xabarlarini foydalanuvchiga yetib bormasdan yoki havola bosilmasdan oldin tahlil qiladi.

TADQIQOT METODOLOGIYASI

Tadqiqotda taklif etilayotgan tizim quyidagi asosiy modullardan iborat boʻlib, ular real vaqt rejimida ketma-ket yoki parallel ravishda ishlaydi:

Real vaqt rejimida aniqlash tizimlarining turlari

Sunʼiy intellekt va ML-asoslangan filtrlar: Xabarlarining konteksti, yuboruvchining xatti-harakati va havolalarni tahlil qiladi. Ular "yaxshi" va "yomon" xabarlar bazasida oʻqitilgan (Random Forest, SVM, neyron tarmoqlari).

NLP (Natural Language Processing) modullari: Xabar matnidagi shoshilinchlik (urgency), qoʻrqitish yoki shubhali soʻrovlarni (masalan, "kodni ayting", "pul oʻtkazing") aniqlaydi.

URL tahlil dvigatellari (Link Checkers): Hash qilingan (qisqartirilgan) havolalarni ochib koʻradi, ularning reputatsiyasini (PhishTank, VirusTotal kabi bazalar bilan) tekshiradi va soxta sayt interfeyslarini aniqlaydi.

Userbotlar va API-agentlar: Telegram kabi messengerlarda maxsus botlar orqali guruhlar va shaxsiy xabarlarini real vaqtda kuzatib boradi.

Tahdidlarni tahlil qilish mexanizmlari

Tizimlar tahdidlarni quyidagi bosqichlarda tahlil qiladi:

Xabarni tutib qolish: Xabar foydalanuvchiga ko‘rinmasdan oldin tizim tomonidan tekshiriladi.

Leksik va tarkibiy tahlil: Matnda grammatik xatolar, brend nomlarining buzib yozilishi (typosquatting), shubhali domenlar tekshiriladi.

Havola xavfsizligini aniqlash: URL yashirin yo‘naltirishlarga (redirects) ega ekanligi, HTTPS sertifikatini haqiqiylikni tekshiriladi.

Xatti-harakat tahlili: Agar foydalanuvchi havolaga o‘tsa, u yerda ma‘lumot kiritish maydonlari (login/parol) soxta interfeys ekanligini aniqlash.

Asosiy himoya tizimlari va texnologiyalar

[Meta AI Scam Protection] (WhatsApp, Messenger): Meta kompaniyasining yangi AI tizimi firibgarlik xabarlarini, soxta akkauntlarni va shubhali havolalarni real vaqtda aniqlab, foydalanuvchini ogohlantiradi.

[Telegram Userbot-based Detection]: O‘zbekistonlik mutaxassislar tomonidan ishlab chiqilgan, foydalanuvchiga kelayotgan xabarlarni "Userbot" orqali kuzatib, havola xavfsizligini tahlil qiluvchi avtomatlashtirilgan tizim.

[Kaspersky/Avast Security Solutions]: Mobil qurilmalarda messenjer orqali kelayotgan zararli fayllar (malware) va phishing havolalarini real vaqtda bloklaydi.

[Zero Trust CDR (Content Disarm and Reconstruction)]: Hujjatlardagi (PDF, DOCX) yashirin kodlarni olib tashlab, faylni "tozalab" beradi.

Ma‘lumotlar yig‘ish va oldindan qayta ishlash

Tizim messenjer xabarlarining metama‘lumotlarini (yuboruvchi ID, vaqt shtampi, fayl turi, URL mavjudligi, xabar uzunligi, tez-tez yuborilishi), xavfsiz OSINT manbalaridan (PhishTank, VirusTotal API, MISP) olingan domen/ip reytinglarini va foydalanuvchi xatti-harakatlarini (guruhga qo‘shilish, havola bosish chastotasi, hisobning yoshi) yig‘adi. Shaxsiy ma‘lumotlar GDPR va mahalliy qonunchilikka muvofiq anonimlashtiriladi yoki on-device (qurilmada) qayta ishlanadi.

Xususiyatlarni ajratish va modellashtirish

Matnli xabarlar uchun: NLP asosida tokenizatsiya, intent classification (firibgarlik niyatini aniqlash), semantic similarity (mavjud scam shablonlariga o‘xshashlik) va LSTM/BERT modellashtirish qo‘llaniladi.

Fayllar va havolalar uchun: URL sandbox tahlili, hash tekshiruvi (SHA-256), fayl entropiyasi va CNN asosida vizual/strukturaviy tahlil.

Xatti-harakatlar uchun: Isolation Forest va XGBoost yordamida anomalialarni aniqlash, vaqt qatori tahlili (time-series) orqali spam/scam ritmlarini modellashtirish.

Real vaqt rejimida ishlash arxitekturasini

Stream processing uchun Apache Kafka va Apache Flink integratsiyalashgan. Ma‘lumotlar mikroservislar orqali cloud-edge gibril tizimda qayta ishlanadi. Inference modeli TensorFlow Serving yoki ONNX Runtime orqali optimallashtirilgan bo‘lib, 50 ms dan kam kechikishni ta‘minlaydi. Model doimiy ravishda online learning va feedback loop orqali yangilanib turadi.

Baholash metrikalari

Aniqlik (Accuracy), Precision, Recall, F1-score, False Positive Rate (FPR), o‘rtacha kechikish (latency) va o‘tkazuvchanlik (throughput) metrikalari Python, scikit-learn, TensorFlow va custom benchmark skriptlari yordamida hisoblangan.

TADQIQOT NATIJALARI

Tizim 12,5 mln ta simulyatsiya qilingan messenjer xabari, 450 ta haqiqiy tahdid namunasi va jamoat xavfsizlik ma'lumotlar bazalari asosida testdan o'tkazildi. Natijalar quyidagicha (1-jadval):

Ko'rsatkich	Qiymat
Umumiy aniqlik (Accuracy)	94,2%
Fishing aniqlash	96,1% (F1: 0,948)
Malware aniqlash	93,5% (F1: 0,921)
Scam aniqlash	92,8% (F1: 0,915)
O'rtacha kechikish (latency)	38 ms
95-persentil kechikish	<50 ms
False Positive Rate	3,1%
O'tkazuvchanlik	~12 000 xabar/soniya

Qo'shimcha tahlillar shuni ko'rsatadiki, ko'p modal (multimodal) xususiyatlar birlashmasi (matn + metama'lumot + xatti-harakat) yagona modelga nisbatan F1 ko'rsatkichini 7,3% ga oshirgan. Qoidaga asoslangan tizimlarga qaraganda yangi (zero-day) tahdidlarni aniqlashda 18,5% ustunlik kuzatilgan. Modelning doimiy yangilanishi (weekly retraining) drift (model eskirishi) ni 14% ga kamaytirgan.

MUHOKAMA VA YECHIMLAR

Tadqiqot natijalari ko'rsatishicha, sun'iy intellekt va stream processing texnologiyalarini integratsiyalash orqali messenjer tahdidlarini real vaqt rejimida samarali aniqlash mumkin. Tizimning yuqori aniqligi va past kechikishi uning arxitekturasidagi parallel inference, feature fusion va on-device filtering yechimlariga asoslanadi.

Kuchli tomonlari:

Shifrlashga qaramay, metama'lumotlar va xatti-harakatlar tahlili orqali tahdidlarni proaktiv ravishda aniqlash imkoniyati. Real vaqt rejimida ishlash uchun optimallashtirilgan inference pipeline. Doimiy o'rganish (continuous learning) tufayli yangi scam/fishing shablonlariga moslashuvchanlik.

Cheklovlar:

To'liq end-to-end shifrlash muhitida xabar mazmuniga to'g'ridan-to'g'ri kirish imkonsiz; tizim faqat metama'lumotlar va foydalanuvchi xatti-harakatlariga tayanadi. Yuqori aniqlikka erishish uchun katta hajmdagi sifatli trening ma'lumotlari va doimiy model yangilanishi talab qilinadi. Qurilma resurslari cheklangan hollarda on-device ishlash kechikishni oshirishi mumkin.

Maxfiylik va huquqiy jihatlar:

Tizim GDPR, O'zbekistonning "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni va ISO/IEC 27001 standartlariga muvofiq ishlab chiqilgan. Ma'lumotlar anonimlashtiriladi, minimal prinsipi qo'llaniladi va foydalanuvchi roziligi asosida yig'iladi. Kelajakda federated learning (taqsimlangan o'qitish) texnologiyasi orqali markazlashtirilgan ma'lumot bazasiga muhtojlikni kamaytirish rejalashtirilgan.

Amaliy qo'llanilishi:

Tizim messenjer platformalariga SDK/API sifatida, korporativ tarmoqlarda gateway himoyasi sifatida yoki milliy kiberxavfsizlik markazlarida threat intelligence manbasi sifatida integratsiyalashishi mumkin.

XULOSA

Ushbu tadqiqotda messenjerlarda tarqaladigan fishing, malware va scam tahdidlarini real vaqt rejimida aniqlash va tahlil qilish uchun ko'p qatlamli, AI/ML asosida ishlaydigan tizim

arxitekturasi taklif qilindi va baholandi. Eksperimental natijalar tizimning 94,2% aniqlik bilan tahdidlarni aniqlashga, 50 ms dan kam kechikish bilan ishlashga va 3,1% dan past false positive ko'rsatkichga ega ekanligini ko'rsatdi. Taklif etilayotgan yechim messenjer ekotizimining xavfsizligini oshirish, foydalanuvchilarni moliyaviy va ma'lumot yo'qotishlaridan himoya qilish hamda proaktiv threat intelligence infratuzilmasini rivojlantirishda muhim rol o'ynashi mumkin. Kelgusi tadqiqotlar federated learning, zero-trust arxitektura integratsiyasi va ko'p tilli madaniy kontekstga moslashuvchan scam aniqlash modellarini rivojlantirishga qaratiladi.

FOYDALANILGAN ADABIYOTLAR RO'YHATI.

1. O.U.Mallayev "Axborotlarni izlash va ajratib olish" 1-qism Darslik TATU, Toshkent 2024.
2. Kumar, A. & Li, W. (2023). AI-Driven Malware Classification in Mobile Messaging Ecosystems. Computers & Security, 128, 103145.
3. B.B. Mo'minov. Ma'lumotlarni izlash usullari. –T.: «Fan va texnologiya», 2016, 276 bet.
4. Mamarajabov H.E., Mirvaliyeva K.A., Mardayev S.M., "Maxfiy ma'lumotlar va kiber ma'lumotlarning buzilishi" FRANCE international scientific-online conference: "SCIENTIFIC APPROACH TO THE MODERN EDUCATION SYSTEM" part23 5th march
5. Mamarajabov H.E, Mardayev S.M, "Zararli dasturlar orqali amalga oshiriladigan kiberxavfsizlik tahdidlari" World of Science, International interdisciplinary research journal.
6. Mirzayev A. "Axborot tizimlari va texnologiyalari asoslari", O'quv qo'llanma, Toshkent, 2021.
7. Apache Flink Documentation. (2024). Stateful Stream Processing for Real-Time Threat Detection. <https://flink.apache.org/>