TELEGRAM MUHITIDA PHISHING HAVOLALARNI REAL VAQT REJIMIDA ANIQLASH ALGORITMI

Saydirasulov Nozimjon
Farg‘ona davlat texnika universiteti magistranti
Oksana Porubay
Farg‘ona davlat texnika universiteti “Dasturiy injiniring va Kiberxavfsizlik” kafedrasi dotsenti

Annotatsiya. Ushbu maqolada Telegram messenjeri muhitida phishing havolalarni real vaqt rejimida aniqlashga qaratilgan avtomatlashtirilgan tizim ishlab chiqish masalasi ko‘rib chiqiladi. Taklif etilgan tizim userbot orqali foydalanuvchilardan kelayotgan xabarlarni kuzatadi, ularda mavjud havolalarni aniqlaydi va ularni haqiqiy yoki soxta sifatida tasniflaydi. Tizimda ikkita asosiy modul joriy etilgan: 1- havola xavfsizligini aniqlash moduli va 2- matn tahlil moduli. Ikkinchi modul BERT (Bidirectional Encoder Representations from Transformers) modeli yordamida xabar mazmunini phishingga oidlik darajasini baholaydi.

Kalit so‘zlar: Telegram, phishing, BERT, userbot, real vaqt, havola tahlili, kiberxavfsizlik.

Аннотация. В данной статье рассматривается разработка автоматизированной системы обнаружения фишинговых ссылок в мессенджере Telegram в режиме реального времени. Предложенная система с использованием userbot отслеживает входящие сообщения пользователей, выявляет содержащиеся в них ссылки и классифицирует их как легитимные или вредоносные. В системе реализованы два основных модуля: 1) модуль анализа безопасности ссылок и 2) модуль анализа текста сообщения. Второй модуль основан на модели BERT (Bidirectional Encoder Representations from Transformers), которая позволяет оценивать степень принадлежности текста к фишинговому контенту на основе семантического анализа.

Ключевые слова: Telegram, фишинг, BERT, userbot, реальное время, анализ ссылок, кибербезопасность.

Abstract. This article presents the development of an automated system for detecting phishing links in the Telegram messaging environment in real time. The proposed system utilizes a userbot to monitor incoming user messages, identify embedded URLs, and classify them as legitimate or malicious. The system consists of two main modules: (1) a URL security analysis module and (2) a text analysis module. The second module is based on the BERT (Bidirectional Encoder Representations from Transformers) model, which evaluates the semantic content of messages to determine their likelihood of being phishing-related.

ISSN 3030-3907

Keywords: Telegram, phishing, BERT, userbot, real-time, URL analysis, cybersecurity.

KIRISH.

Hozirgi kunda raqamli xavfsizlik masalalari axborot texnologiyalari rivojining ajralmas qismiga aylangan. Ijtimoiy tarmoqlar va messenjerlar, xususan Telegram**,** foydalanuvchilar o‘rtasida eng ommabop aloqa vositalaridan biri sifatida keng qo‘llanmoqda. Shu bilan birga, bu muhitda kiberjinoyatchilar tomonidan foydalanuvchilarning ishonchidan foydalanib, phishing (soxta havolalar orqali ma’lumot o‘g‘irlash) hujumlarini amalga oshirish holatlari ham ko‘paymoqda. Phishing havolalar ko‘pincha rasmiy ko‘rinishga ega bo‘lib, foydalanuvchini firibgarlik sahifalariga yo‘naltiradi va natijada foydalanuvchi parol, login yoki moliyaviy ma’lumotlarini yo‘qotadi. Shu sababli, Telegram muhitida real vaqt rejimida phishing havolalarni aniqlash va foydalanuvchini himoya qilish muhim masalalardan biridir.

Mazkur tadqiqotda userbot asosida ishlovchi, foydalanuvchilarning xabarlarini avtomatik kuzatib boruvchi va ulardagi havolalarni xavfsizlik nuqtai nazaridan tekshiruvchi tizim taklif etiladi. Tizim shuningdek BERT (Bidirectional Encoder Representations from Transformers) modeli yordamida xabar matnini tahlil qilib, unda phishingga oid ifodalar mavjudligini aniqlaydi. Ushbu yondashuv Telegram guruhlarida va kanallarida avtomatlashtirilgan himoya mexanizmini yaratish imkonini beradi.

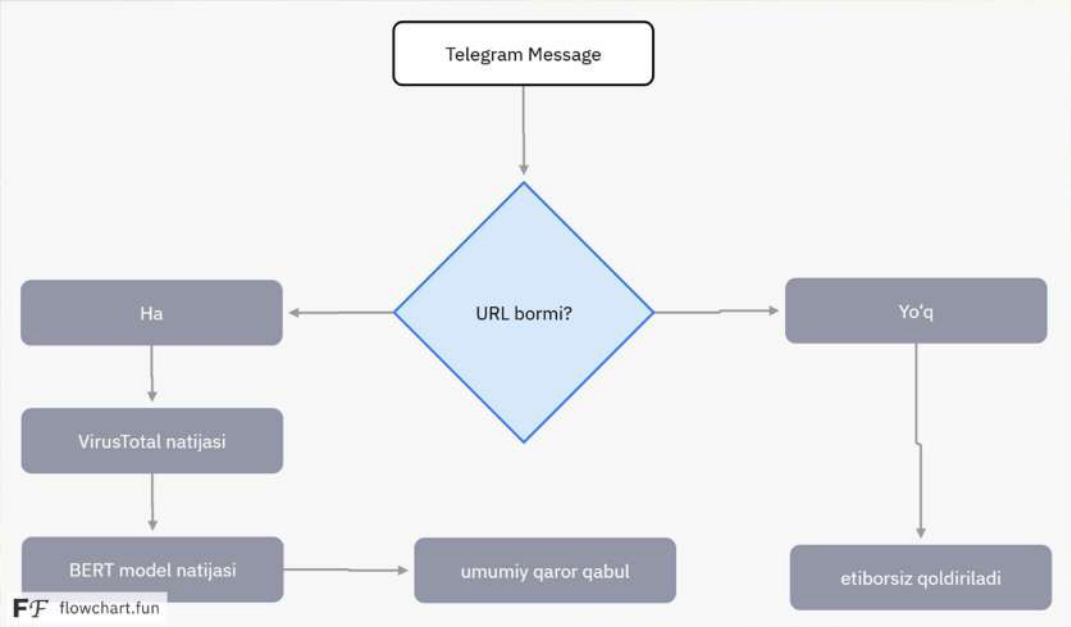
METODOLOGIYA. Mazkur tadqiqotning asosiy maqsadi — Telegram muhitida phishing havolalarni real vaqt rejimida avtomatik aniqlash va foydalanuvchini himoya qilishga qaratilgan algoritmni ishlab chiqishdir. Tizim userbot, havola tahlili, BERT asosidagi semantik analiz, va reaktiv xavfsizlik mexanizmi kabi asosiy modullardan iborat. Quyida har bir modulning ishlash prinsipi, texnik yechimi va baholash mezonlari batafsil bayon etiladi.

1. Umumiy arxitektura

Tizim Telegram tarmog‘idagi xabarlar oqimini real vaqt rejimida kuzatadi. Har bir yangi xabar quyidagi ketma-ket bosqichlar orqali qayta ishlanadi:

1. Xabarni olish
2. URL aniqlash va tahlil qilish
3. Matnni semantik tahlil qilish
4. Natijani baholash va avtomatik chora ko‘rish

ISSN 3030-3907



1-rasm. Telegram platformasida phishing havolalarni aniqlash tizimi ishlash blok sxemasi

Ushbu bosqichlarning barchasi Python tilida ishlab chiqilgan modullar orqali amalga oshiriladi. Har bir jarayon asinxron usulda bajariladi, bu esa real vaqt (real-time) ishlash imkonini beradi.

URL mavjud	VirusTotal (VT)	BERT natijasi	Yakuniy qaror
0	–	–	Tekshirilmaydi
1	1	0	**Phishing**
1	0	1	**Phishing**
1	1	1	**Phishing**
1	0	0	Xavfsiz

2-rasm.Tizimning umumiy qaror qabul qilish jadvali

2. Ma’lumot yig‘ish va userbot mexanizmi

Userbot — Telegram API bilan to‘g‘ridan-to‘g‘ri ishlaydigan avtomatik foydalanuvchi hisobidir. U kanallar yoki guruhlarda paydo bo‘ladigan yangi xabarlarni kuzatib boradi. Buning uchun Telethon kutubxonasidan foydalaniladi, chunki u async (asinxron) ishlash imkoniyatiga ega va bir vaqtning o‘zida yuzlab xabarlarni qayta ishlashi mumkin.

Har bir yangi xabar uchun quyidagi jarayonlar bajariladi:

1. Foydalanuvchi identifikatori, vaqt tamg‘asi va xabar matni bazaga yoziladi.
2. Xabar tarkibida URL borligi tekshiriladi.

ISSN 3030-3907

3. Agar havola aniqlansa, u keyingi tahlil moduliga uzatiladi.
4. Shu tarzda tizim real vaqtli oqim asosida ishlaydi, ya'ni foydalanuvchi xabari kelishi bilanoq tekshiruv boshlanadi.

3. Matnni BERT modeli orqali tahlil qilish

Phishing xabarlar faqatgina havola orqali emas, balki matn mazmuni orqali ham aniqlanishi mumkin. Shu sababli, tadqiqotda BERT (Bidirectional Encoder Representations from Transformers) modelidan foydalangan holda xabar matnlarini semantik jihatdan tahlil qilish yondashuvi taklif etildi. Ushbu yondashuv xabar ichidagi yashirin phishing niyatlarini, manipulyativ ifodalarni va soxta chaqiriqlarni aniqlashda yuqori aniqlik beradi.

Matnli ma'lumotlarni modelga mos shaklga keltirish jarayonida mBERT'ning standart tokenizeridan foydalanildi. Tokenizatsiya jarayoni ikki yo'nalishli kontekstni hisobga olgan holda amalga oshirildi, bu esa so'zlarning faqat ketma-ketlikdagi o'rnini emas, balki ularning umumiy ma'no bog'lanishini ham inobatga olish imkonini berdi. Har bir xabar maksimal uzunlikka moslab kesildi yoki to'ldirildi va model kirishiga embedding ko'rinishida uzatildi.

Modelni o'qitish jarayonida tasniflash vazifasi qo'yildi va chiqish qatlamida fishing, spam yoki oddiy xabar sinflaridan birini bashorat qilish amalga oshirildi. Yo'qotish funksiyasi sifatida ko'p sinfli tasniflash uchun mos bo'lgan kross-entropiya funksiyasi tanlandi, optimallashtirish esa AdamW algoritmi orqali bajarildi. Model bir nechta epox davomida o'qitilib, har bir epox yakunida validatsiya ma'lumotlari asosida baholandi.

Fishing kontekstlarni o'rganish jarayonida model xabar matnida yashirin tarzda berilgan ijtimoiy muhandislik elementlarini aniqlashga moslashtirildi. Bu yondashuv an'anaviy kalit so'zlarga asoslangan filtrlashdan farqli ravishda, matnning umumiy semantik mazmunini hisobga olish imkonini berdi. Modelni baholash jarayonida aniqlik, aniqlik darajasi, to'liqlik va F1-ko'rsatkichlar asosiy mezon sifatida tanlandi va barcha hisob-kitoblar test ma'lumotlar to'plami asosida amalga oshirildi.

mBERT modelida kirish ketma-ketligi $X = (x_1, x_2, \dots, x_n)$ token embeddinglar orqali vektorlarga o'tkaziladi va har bir Transformer qatlamida o'z-o'ziga e'tibor mexanizmi quyidagi formula asosida hisoblanadi:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

bu yerda

$Q=XW_Q$

$K=XW_K$

$V=XW_V$

ISSN 3030-3907

$W_Q, W_K, W_V \in$ R o‘rganiladigan parametrlar.

Tasniflash bosqichida mBERT modelining oxirgi qatlamidan olingan **[CLS] token** yashirin holati h_{CLS} asosida sinf ehtimolliklari hisoblanadi:

$$\hat{y} = \text{softmax}(Wh_{\text{CLS}} + b)$$

Modelni o‘qitishda yo‘qotish funksiyasi sifatida ko‘p sinfli kross-entropiya funksiyasi qo‘llaniladi:

$$\mathcal{L} = -\sum_{i=1}^{C} y_i \log(\hat{y}_i)$$

y_i — haqiqiy yorliq,

$\hat{y}_i$— model bashorat qilgan ehtimollik.

Ushbu formulalar asosida mBERT modeli fishing xabarlaridagi yashirin semantik va kontekstual belgilarni o‘rganadi hamda matnlarni aniq sinflarga ajratadi.

NATIJALAR. Ushbu tadqiqot doirasida Telegram muhitida phishing havolalarni real vaqt rejimida aniqlashga mo‘ljallangan avtomatlashtirilgan bot ishlab chiqildi va tajribaviy sinovdan o‘tkazildi. Sinov jarayonida bot 56 nafar foydalanuvchi tomonidan faol foydalanildi va foydalanuvchilarning shaxsiy hamda guruh suhbatlariga kelib tushgan xabarlar real vaqt rejimida tahlil qilindi.

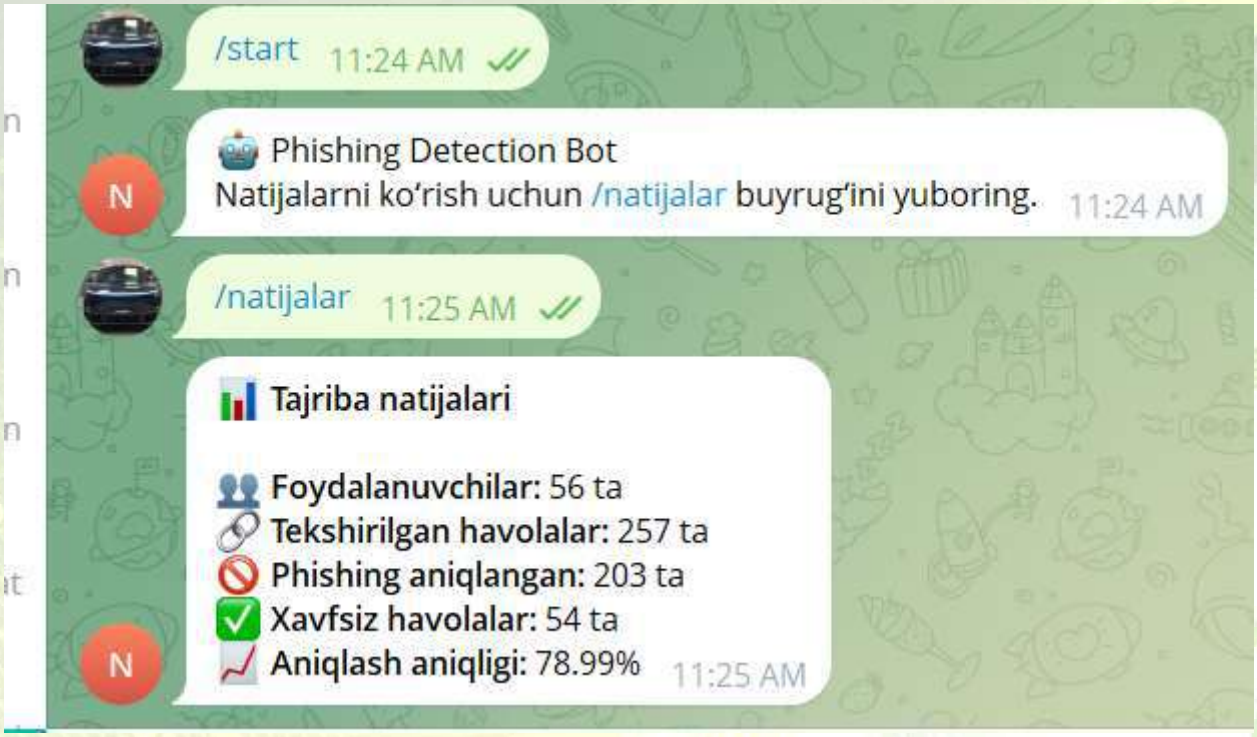
Tajriba davomida jami 257 ta havola tekshirildi. Havolalar URL strukturasi, domen ishonchliligi va shubhali belgilar asosida dastlabki filtrdan o‘tkazildi. Natijada 203 ta havola phishing sifatida aniqlanib, bot tomonidan avtomatik tarzda o‘chirib tashlandi. Qolgan 54 ta havola xavfsiz deb topildi va foydalanuvchilarga yetkazilishiga ruxsat berildi.

Phishing havolalarni aniqlash samaradorligini baholash maqsadida aniqlik ko‘rsatkichi hisoblandi. Tajriba natijalariga ko‘ra, tizimning aniqlash aniqligi 78.99 % ni tashkil etdi. Bu ko‘rsatkich real vaqt rejimida ishlaydigan avtomatlashtirilgan himoya mexanizmi uchun qoniqarli natija hisoblanadi.

Shuningdek, tizimning ishlash tezligi tahlil qilinib, har bir yangi xabar o‘rtacha bir necha soniya ichida tekshirildi. Bu holat foydalanuvchini phishing hujumlaridan tezkor himoya qilish imkonini berdi va Telegram platformasi faoliyatiga sezilarli yuklama keltirib chiqarmadi.

Olingan natijalar shuni ko‘rsatdiki, Telegram muhitida havola tahlili asosida ishlovchi avtomatlashtirilgan bot phishing havolalarni samarali aniqlash va ularni real vaqt rejimida bartaraf etish imkoniyatiga ega. Ushbu yondashuv foydalanuvchilarning axborot xavfsizligini oshirishda amaliy ahamiyatga ega ekanligi tajribaviy jihatdan tasdiqlandi.

ISSN 3030-3907



3-rasm. telegram bot orqali olingan natijalar tahlili

1-jadval.

Userbot orqali aniqlangan zararli havolalar tahlili

Umumiy foydalanuvchilar	56 ta
Tekshirilgan havolalar	257 ta
Zararli deb topilgan havolalar	203 ta
Xavfsiz deb topilgan havolalar	54 ta
Zararli havolalar foiz ko‘rinishi	78 %

FOYDALANILGAN ADABIYOTLAR

1. Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL-HLT)*, 4171–4186. https://doi.org/10.18653/v1/N19-1423

2. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 30, 5998–6008.

3. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, 117, 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

4. Aljofey, A., Jiang, Q., Rasool, A., Chen, H., & Liu, Y. (2020). An effective phishing detection model based on character level convolutional neural network from URL. *Electronics*, 9(9), 1514. https://doi.org/10.3390/electronics9091514

ISSN 3030-3907

5. Adebowale, M. A., Lwin, K. T., Sanchez, E., & Hossain, M. A. (2019). Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text. *Expert Systems with Applications*, 115, 300–313. https://doi.org/10.1016/j.eswa.2018.07.052
6. Feng, S., Xie, R., Yu, H., & Liu, Z. (2021). Phishing detection on social media platforms using deep learning models. *IEEE Access*, 9, 152–163. https://doi.org/10.1109/ACCESS.2021.3051234
7. Telegram. (2023).

ISSN 3030-3907