МРНТИ 27.25.19 **https://doi.org/10.58805/kazutb.v.1.30-1213**

ЖЕЛІ АРҚЫЛЫ ЖАЛҒАН КОНТЕНТТІ ТАСЫМАЛДАУДЫ ІЗДЕУ ҮШІН ЖЕЛІЛІК ТРАФИКТІ ТАЛДАУ

З.А. Сарсембаева, Г.И. Аймичева, А.Е. Назырова
Л.Н.Гумилев атындағы Еуразия Ұлттық университеті, Астана, Қазақстан
Корреспондент-автор: 040203650680@enu.kz

Цифрлық технологиялар мен жасанды интеллекттің қарқынды дамуы жалған ақпарат таратудың жаңа мүмкіндіктерін ашты. Қазіргі уақытта жалған контентті анықтауға бағытталған зерттеулер көбінесе визуалды талдаумен шектеледі, ал желі деңгейінде оны анықтаудың тиімді әдістері жеткіліксіз зерттелген. Сондықтан бұл зерттеу жұмысының негізгі мақсаты желілік трафикті талдау арқылы жалған контентті, соның ішінде дипфейк мазмұнын анықтаудың тиімді техникалық әдістерін ұсыну болып табылады. Бұл жұмыста HTTP-трафикті талдау, файлдарды автоматты түрде шығару, MesoNet нейрондық желі моделі арқылы дипфейктерді анықтау әдістері қолданылды. Зерттеу барысында Scapy, PyTorch және Docker технологиялары пайдаланылды. Нәтижелер көрсеткендей, ұсынылған әдіс дипфейк-контентті желілік трафик деңгейінде нақты уақыт режимінде жоғары дәлдікпен анықтай алады. Жүйе қауіпті контентті автоматты түрде анықтап, Telegram арқылы жедел хабарландыру жібереді, бұл ақпараттық қауіпсіздікті қамтамасыз етуде үлкен практикалық мәнге ие.

Түйін сөздер: жалған контент, дипфейктер, ақпараттық қауіпсіздік, желілік трафикті талдау, нейрондық желілер, Scapy, MesoNet, автоматты талдау, дезинформация, цифрлық криминалистика.

АНАЛИЗ СЕТЕВОГО ТРАФИКА ДЛЯ ПОИСКА РАСПРОСТРАНЕНИЯ ЛОЖНОГО КОНТЕНТА ЧЕРЕЗ СЕТЬ

З.А. Сарсембаева, Г.И. Аймичева, А.Е. Назырова
Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан,
e-mail: 040203650680@enu.kz

Стремительное развитие цифровых технологий и искусственного интеллекта открыло новые возможности для распространения ложной информации. Особенно в последние годы широко распространяется дипфейк-контент, не являющийся реальным, но визуально убедительный. В настоящее время исследования, направленные на выявление ложного контента, в основном ограничиваются анализом на визуальном уровне, тогда как методы его эффективного обнаружения на сетевом уровне изучены недостаточно. В связи с этим основной целью исследования является предложение эффективных технических подходов к выявлению ложного контента, включая дипфейки, посредством анализа сетевого трафика. В работе использовались методы анализа HTTP-трафика, автоматического извлечения файлов и определения дипфейков с помощью нейронной сети MesoNet. В ходе исследования применялись технологии Scapy, PyTorch и Docker. Результаты показали, что предложенный метод способен выявлять дипфейк-контент на уровне сетевого трафика в режиме реального времени с высокой точностью. Система автоматически определяет опасный контент и оперативно отправляет уведомления через Telegram, что имеет большое практическое значение для обеспечения информационной безопасности.

Ключевые слова: ложный контент, дипфейки, информационная безопасность, анализ сетевого трафика, нейронные сети, Scapy, MesoNet, автоматический анализ, дезинформация, цифровая криминалистика.

NETWORK TRAFFIC ANALYSIS FOR DETECTING THE DISTRIBUTION OF FALSE CONTENT OVER THE NETWORK

Z.A. Sarsembayeva✉, G.I. Aimicheva, A.Ye. Nazyrova
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
e-mail: 040203650680@enu.kz

The rapid development of digital technologies and artificial intelligence has opened up new opportunities for the dissemination of false information. In recent years, deepfake content, which is not authentic but visually convincing, has become widespread. Current studies on detecting false content are mostly limited to visual-level analysis, while effective methods for identifying it at the network level remain insufficiently explored. Therefore, the main objective of this research is to propose effective technical approaches for detecting false content, including deepfakes, through network traffic analysis. This study applied HTTP traffic analysis, automatic file extraction, and deepfake detection using the MesoNet neural network model. The research utilized Scapy, PyTorch, and Docker technologies. The results demonstrated that the proposed method can accurately detect deepfake content at the network traffic level in real time. The system automatically identifies malicious content and promptly sends alerts via Telegram, which has significant practical value for ensuring information security.

Keywords: false content, deepfakes, information security, network traffic analysis, neural networks, Scapy, MesoNet, automated analysis, disinformation, digital forensics.

Кіріспе. Қазіргі таңда жасанды интеллект пен ақпараттық технологиялардың дамуы арқасында жалған ақпараттың цифрлық кеңістікте таралу жылдамдығы мен күрделілігі күннен күнге артуда. Жалған контент тек әлеметтік желілерде ғана емес, сонымен қатар – форумдар, хабарламалар жүйесі және заңды сайттар арқылы да таралуда. Бүгінде жалған ақпарат тек мәтін немесе бейне түрінде ғана емес, мультимедиялық пішінде, яғни суреттер мен аудиофайлдар арқылы да берілуі мүмкін. Көзге шынайы көрінетін, бірақ шын мәнінде жалған болып келетін және адам өміріне, беделіне нұқсан келтіретін контентті алдын ала анықтап, оның таралуын тоқтату қазіргі кездегі ақпараттық қаіпсіздіктің басты мәселелерінің бірі.

Жалған контентті танудағы зерттеулер көбіне визуалды ерекшеліктерді анықтауға бағытталған, ал оларды ерте кезеңде анықтап, оның таралуына жол бермеу туралы зерттеулер қазіргі кезде аса көп қарастырылмаған және де тапшылық етуде. Бұл ақпараттық қауіпсіздік саласындағы маңызды кемшіліктердің бірі.

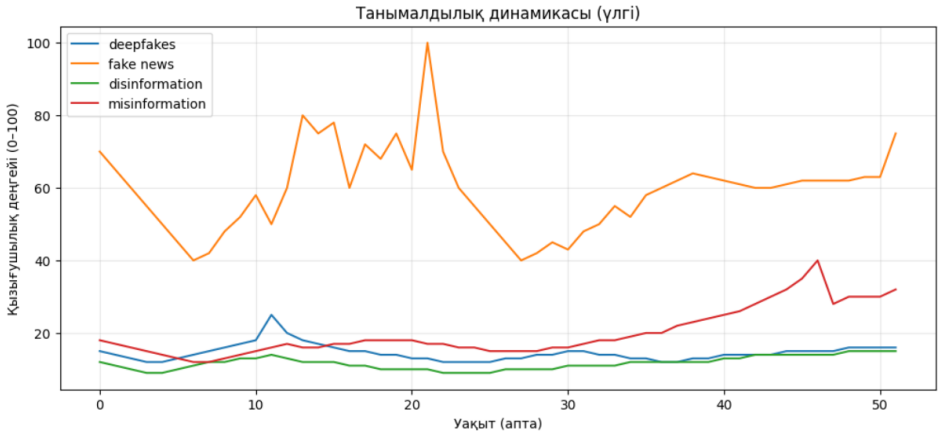
Осы себептен, бұл зерттеу жұмысының басты мақсаты – жалған контентті желілік трафикті талдау арқылы анықтау әдістерін ұсыну. Негізгі зерттеу сұрағы: желілік трафикті талдау арқылы жалған контенттің таралуын қалай тоқтатуға болады?

Әдебиетке шолу. Ақпараттық кеңістіктегі жалған контенттің таралуы қоғамдағы пікірді бұрмалап, халықтың шешім қабылдауына ықпал етеді. Соңғы зерттеулер көрсеткендей, психологиялық тұрғыдан әсерлі жалған контент адамдар арасында шыңайы ақпаратқа қарағанда 70%-ға жылдам таралады.

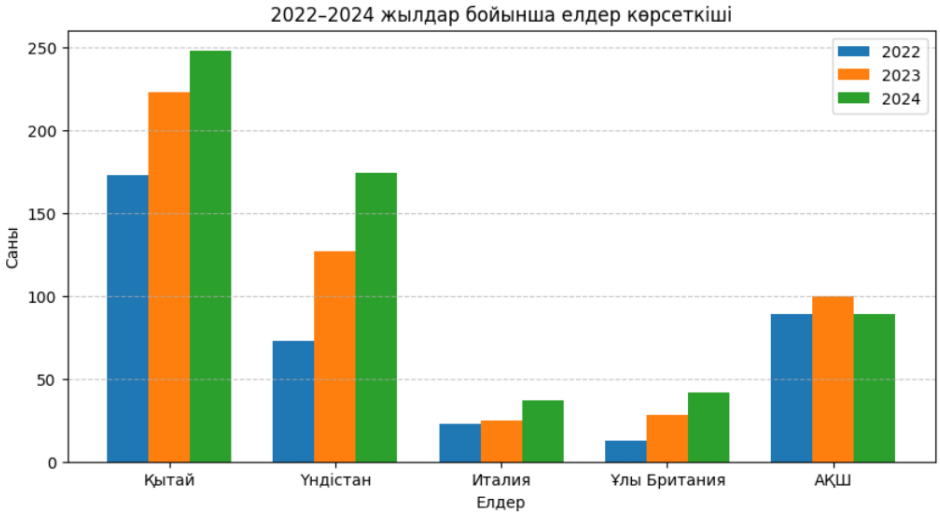
Google trends (https://trends.google.com/trends/) деректеріне сәйкес, «Fake news» (жалған жаңалықтар), «deepfakes» (жасанды бейнелер), «disinformation» (әдейі таралған жалған ақпарат) және «misinformation» (білместіктен таралған жалған ақпарат) сияқты сұраныстар адамдар арасында тұрақты қызығушылық тудыруда. Мұндай қызығушылықты әсіресі, саяси, әлеуметтік және экономикалық оқиғалар кезінде байқауға болады. Бұл халықтың жалған ақпаратқа алданып қалуына деген қорқынышын және дезинформация қаупын түсінуін көрсетеді.

Соңғы бірнеше жыл ішінде бұл терминдер бойынша іздеу белсенділігі жаһандық деңгейде ғана емес, Қазақстанда да айқын өсуде. Бұд құбылыс дезинформацияның тек халықаралық ауқымдағы мәселе екенін көрсетеді. Осы орай-

да, жалған контентпен күресуде тиімді техникалық құралдар мен әдістерді әзірлеу қажеттілігі барған сайын айқындала түсуде.



1-сурет. Google Trends мәліметтері бойынша жалған ақпарат және deepfakes тақырыптарына қызығушылық



2-сурет. Дипфейктер мен жасанды интеллект тақырыбы бойынша ғылыми жарияланымдардың елдер бойынша белсенділігі

Бұл зерттеу тақырыбы ғылыми ортада да кең танымалдылыққа ие. SciVal платформасының бибилеометриялық талдау деректеріне сүйінетін болсақ, 2022-2024 жылдар арасында дипфейк, терең оқыту және жасанды интеллект туралы мақалалар саны бұрынғымен қарағанда әрдеқайда артып келуде. Әсіресе бұл мәселеге Қытай, Үндістан, АҚШ, Италия және Ұлыбритания елдерінің ғалымдары ерекше көңіл бөлген. Жарияланымдар саны бойынша Қытай (644), Үндістан (374) және АҚШ (278) елдері көш бастап тұр. Ал Италия (85) және Ұлыбритания (83) елдері бір-бірінен қалыспай, алғашқы бестікті түйіндейді (сурет-2).

Материалдар мен әдістер. Желілік трафикті талдауға арналған NTMA әдістемесі арқылы жалған контентті анықтау. Желілік трафикті талдау – ақпараттық қауіпсіздікті қамтамасыз ететін басты құралдардың бірі. Трафикті талдау арқылы әдеттен тыс нәрселерді (аномалияларды), заңсыз әрекеттерді, фишингтік ша-

буылдарды және жалған ақпаратты тарату арналарын анықтауға болады. Соңғы жылдары әлеуметтік желі арқылы жалған ақпараттың көбеюі және де зиянды бағдарламалардың таралуының өсуіне байланысты бұл талдаудың ғылыми тұрғыдағы маңызы арта түсуде. Желілік құрылымдардың күрделенуі және деректерді шифрлау әдістерінің жетілуі дәстүрлі тексеру құралдарының қолдану аясын шектеп, жаңа тәсілдерді талап етуде. Сондықтан, машиналық оқыту мен терең оқытуға негізделген әдістерді қолдану қажеттілігі артуда.

NTMA (Network Traffic Monitoring and Analysis), яғни желілік трафикті бақылау және талдау – бұл желінің қозғалысын ең ұсақ бөлшектерге дейін бақылауға мүмкіндік беретін әдістер жиынтығы. Бұл тәсіл желінің жұмысын және өнімділігін терең зерттеуге, сондай-ақ пайдаланушылардың желідегі әрекеттерін талдауға мүмкіндік береді [1]. Коммуникациялық жүйелер мен желілер тұрғысынан алғанда NTMA өте маңызды рөл атқарады. Ол желілердің қалай жұмыс істейтінін түсінуге, олардың өнімділігін бақылауға, ресурстарды тиімді пайдалануды, оңтайландыруды және телекоммуникациялық инфрақұрылымды SLA (Service Level Agreement – қызмет көрсету деңгейі туралы келісім) талаптарына сәйкес басқаруға көмектеседі.



3-сурет. NTMA процедурасының құрылымы

Машиналық оқыту мен терең оқыту әдістерін пайдалану арқылы NTMA жүйелері желілік аномалияларды автоматты түрде анықтай алады. Терең оқыту (Deep Learning) белгілерді автоматты түрде шығарып, деректердегі жасырын заңдылықтарды анықтау үшін қолданылады. Бұл технология үлкен көлемдегі деректерді талдау отырып, модельдердің жұмыс тиімділігін арттырады және дәстүрлі машиналық оқыту әдістерінен бір саты жоғары тұрады [1].

NTMA желі ресурстарын басқаруда және қауіпсіздікті қамтамасыз етуде басты құрал болып саналады. Терең оқыту әдістерін пайдалану желі трафигін талдау міндеттерін қазіргі коммуникациялық жүйелердің жоғары жылдамдық пен сенімділік талаптарына сай шешуге көмектеседі.

Машиналық оқыту шифрланған трафикті талдауға NTMA-ны бейімдеуде маңызды рөл атқарады. Әдеттен тыс жағдайларды (аномалияларды) анықтау үшін көбінесе автоэнкодерлер пайдаланылады, олар жүйенің қалыпты міңез-құлқынан ауытқуын бірден байқайды. Сондай-ақ, K-орташа кластерлеу сияқты бақылаусыз әдістерге негізделген кластерлеу трафиктің жаңа үлгілерін табуға ат салысады. Мысалы, автоэнкодерлерді шифрланған ағындарды тексеруге қолдану HTTPS арқылы деректерді жасырын шығары әрекеттерін анықтауға мүмкіндік берді [1,2].

Желілік трафикті талдауда Deep Packet Inspection (DPI) және NetFlow әдістерінің үлесі зор. Бұл әдістердің әрқайсысы желідегі ақпарат ағындарын зерттеуде өзіндік ерекшеліктермен көзге түскен.

Deep Packet Inspection (DPI) - бұл желі арқылы өтетін пакеттердің ішкі мазмұнын толықтай тексеруге мүмкіндік беретін технология. Яғни, қарапайым сөзбен айтқанда, ол тек пакеттің тақырыбын ғана емес, сонымен қатар оның ішкі құрылымында талдайды. DPI-дің басты артықшылықтарының бірі - желідегі заңсыз әрекеттерді, шифрланған трафиктегі күдікті үлгілерді және зиянды бағдарламаларды анықтау қабілеті. Бұл әдіс қауіпсіздік жүйелерінде, атап айтқанда IDS (Intrusion Detection Systems - шабуылды анықтау жүйелері) және IPS (Intrusion Prevention Systems - шабуылды алдын алу жүйелері) белсенді қолданылады [2].

NetFlow - желілік трафиктің құрылымдық си-

паттамаларын талдауға арналған Cisco компаниясы әзірлеген технология. Ол аномалияларды табу үшін трафик ағындарының статистикалық мәліметтерін жинайды. NetFlow - DDos шабуылдарын, ботнеттердің белсенділігін, және фишингтік шабуылдарды айқындауда тиімді болып табылады.

DPI мен NetFlow тәсілдерін бірге қолдану арқасында желілік қауіпсіздікті қамтамасыз ету оң нәтижелер береді. DPI арқылы пакеттердің ішкі мазмұнына назар аударсақ, NetFlow арқылы трафик ағындарының құрылымдық параметрлерін талдап, желідегі күдікті мінез-құлықты анықтауға болады. Осы тәсілдердің бірігуі желідегі заңсыз әрекеттерді, зиянды бағдарламаларды және жалған ақпаратты тарату арналарының белсенділігін жоғары дәлдікпен анықтауға мүмкіндік береді [3].

Көпмодальды тәсілдер дегеніміз – әртүрлі ақпарат түрлерін (мәтін, сурет, бейне, аудио) біріктіріп талдауға негізделген әдістер. Көпмодальды әдістерді пайдалану арқылы жалған ақпаратты таратудың бірнеше негізгі бағыты пайда болған. Біріншіден, әлеуметтік желілер мен жаңалықтарда тек мәтіндік контент ғана емес, сонымен қатар суреттер мен бейнелер белсенді қолданылады. Мұндай медиалық элементтер жалған ақпараттың шыңайлылық деңгейін күшейту мақсатында жасалады [4].

Көпмодальды тәсілдердің желілік криминалистикадағы маңызы зор. Себебі, жалған ақпарат таратушылар көбіне тек бір ғана дереккөзбен шектелмей, бірнеше арнаны бір мезгілде қолданады. Мысалы, әлеуметтік желілердегі жалған жаңалықтар көбінесе мәтін, сурет және бейне форматтарында қатар беріледі және олардың арасында өзара логикалық байланыс болады. Осы байланыстарды толыққанды талдау үшін көпмодальды әдістерді қолданамыз.

Жалған ақпаратты көпмодальды әдістер арқылы анықтауда машиналық оқыту мен терең оқыту әдістері белсенді қолданылады. Бұл әдістер әртүрлі дереккөздерден алынған ақпаратты біріктіруге және олардың арасындағы айырмашылықтарды анықтауға мүмкіндік береді [5].

Бұл бағыттағы негізгі модельдердің бірі - GNN (Graph Neural Networks - графтық нейрондық желілер). GNN ақпараттың таралу жолдарын зерттеп, күмәнді байланыстарды анықтауға көмектеседі. Бұл модельден бөлек, визуалды контентті өңдеу үшін CNN (Convolutional Neural Netwoorks – конволюциялық нейрондық желілер) және мәтіндік және аудиофайлдарды талдау үшін LSTM (Long Short-Term Memory ұзақ мерзімді жады) модельдері қолданылады. Жалған контентті талдауда қолданылатын әдістердің тиімділігі мен тәжірибелік маңызын негіздеу мақсатында [5-7] әдебиеттердегі ғылыми мақалаларға талдау жасалды, нәтижесі 1-кестеде ұсынылған.

Көпмодальды тәчілдерді қолдану кезінде ерекше назар аударуға тұрарлық тағы бір аспект - кросс-модальды сәйкессіздіктерді анықтау. Бұл операциялар әртүрлі ақпарат көздері арасындағы сәйкестікті бағалауға мүмкіндік береді. Мысалы, хабарлама мәтіні бір оқиға туралы, бірақ оған тіркелген бейне басқа оқиға туралы болуы мүмкін. Мұндай айырмашылықтарды автоматты түрде анықтау үшін көпмодальды нейрондық желіліер қолданылады [8].

1-кесте. Көпмодальды терең оқыту архитектураларының сипаттамасы

Архитектура	Сипаттамасы	Қолдану салалары	Жалған контентті анықтаудағы өзектілігі
Көпқабатты персептрон (MLP)	Тығыз қабаттардан тұрады, әр қабат деректердің жаңа түрін береді.	Мәтінді, суретті және дыбысты біріктіру үшін қолданылатын негізгі әдіс.Әр түрлі дереккөздерді синхрондау және олардан алынған ақпаратты біріктіру.	Жалған немесе бұрмаланған мазмұнды көрсететін метадеректердегі ауытқуларды анықтау

Конволюциялық нейрондық желілер (CNN)	Уақыт қатарлары немесе кеңістіктік деректер сияқты тор деректер құрылымдарын өңдеуге арналған, ол жергілікті үлгілерді (мысалы, кластер өлшемі, ұзақтығы) бөлектейді.	Суреттер мен бейнелерді өңдеу, бейнелерді мәтінмен байланыстыру және мазмұн үйлесімділігін тексеру.	Жасанды мазмұнды жеткізуге байланысты орындалатын пакеттік үлгілер мен пайдалы жүктеме шабуылдарында оғаш ауытқуларды анықтау
Рекуррентті нейрондық желілер (RNN)	Деректерді ретімен өңдейді. RNN алдыңғы кірістердің «есту қабілетін» сақтайды, уақыт реттілігін талдау үшін қолайлы етеді.	Мәтіндік және дыбыстық деректерді уақытша байланыстар бойыншы зерттеу, жалған хабарламаларды сұрыптау	Деректер ағынындағы уақытша сәйкессіздіктерді қадағалау арқылы жалған немесе өзгертілген мазмұнды анықтайды
Ұзақ мерзімді жады (LSTM)	RNN-ге ұқсас, градиент жоғалуымен байланысты мәселелерді шешеді. Тізбектердегі ұзақ мерзімді маусымдық тәуелділіктерге мамандандырылған.	Уақыт бойынша деректердің өзгеруін талдау, мәтін мен аудио контент арасындағы байланысты зерттеу	Уақыт өте келе өзгертілген немесе жалған ақпаратқа тән ауытқуды анықтау.
Гейттелген рекуррентті блоктар (GRU)	LSTM-нің жеңілдетілген нұсқасы, есептеу ресурстарын аз талап етеді, бірақ тізбекті деректерді өңдеуде ұқсас қабілеттерге ие	Мәтін, аудио және бейнелерді LSTM-ге қарағанда тезірек талдайды.	Жалған мазмұнды тарату-дағы трафик үлгілеріндегі қарапайым айырмашылықтарды анықтайды.
Автоэнкодерлер	Бақылаусыз оқыту үшін қолайлы архитектура. Кіріс деректерін қысылған көріністерге кодтауға және оларды қайта құруға үйретілген нейрондық желілер	Әртүрлі дереккөздерден алынған ақпаратты қысу және олардың арасындағы заңдылықтарды тану	Қайта құрастырылған деректердің бұрмалануымен байланысты сәйкессіздіктер мен ауытқуларды анықтау
Терең генеративті модельдер	Вариациялық автоэнкодерлер (VAE) және генеративті қарсылас желілер (GAN) сияқты әдістерді қамтиды.	Генеративті модельдерді қолданып, дипфейкті құрады және оны анықтау үшін кері талдау жүргізеді.	Жалған трафикті имитациялау немесе сенімділікті тексеру үшін қарсы нүктелерді жасау үшін үлгілерді үйрету
Гибридті модельдер (CNN-RNN)	CNN кеңістік ерекшеліктерін және RNN уақытша модельдеуін біріктіреді.	Жалған контенттің сәйкестігін сурет, мәтін және аудионы өңдеу арқылы тексереді	Кеңістіктік және уақыттық белгілерді біріктіру арқылы жалған контенттің таралуындағы күрделі заңдылықтарды анықтау
Ансамбльдік модельдер	Бірнеше архитектураның артықшылықтарын пайдалану үшін, оларды бір модельге біріктіреді.	Мәтін,сурет және дыбыс арасындағы үйлесімділікті айқындау үшін бірнеше үлгілердің нәтижелерін біріктіру	Жалған контентті анықтау үшін бірнеше тәсілдерді біріктіріп қолданады.

Көпмодальды тәсілдердің тағы бір маңызды артықшылығы - статистикалық талдау мен мазмұнды бағалау үйлесімі. Бұл тәсіл мазмұнды тарату динамикасын және оның пайдаланушыға әсерін зерттеуге мүмкіндік береді. Әлеуметтік желілердегі тенденцияларды талдай отырып, жалған ақпараттың таралу жылдамдығын және оның аудиториясын анықтауға болады. Бұл талдау тәсілі жалған ақпараттың табиғатын зерттеуге және оның таралуын алдын алуға мүмкіндік береді [9].

Нәтижелер және талқылау. Эксперименттік жұмыстың мақсаты - жалған контентті анықтау үшін желілік трафикті талдауға арналған кешенді шешім құру. Осы мақсатқа жету үшін келесі міндеттер қойылды:

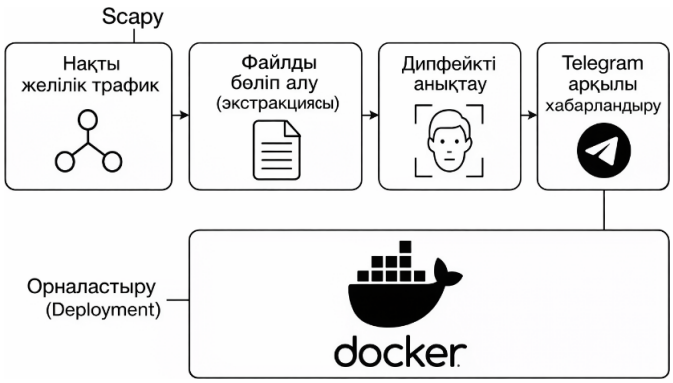
1. HTTP-трафигін сенімді түрде ұстап қалу;

2. Трафиктен автоматты түрде медиафайлдарды бөліп алу;

3. Таңдалған нейрондық желі арқыла медиаконтентті талдау;

4. Күдікті медиафайл табылған жағдайда, Telegram bot арқылы хабарлама жіберу.

Бұл күрделі шешімді жүзеге асыру үшін Scapy, PyTorch және Docker технологиялары таңдалған болатын.

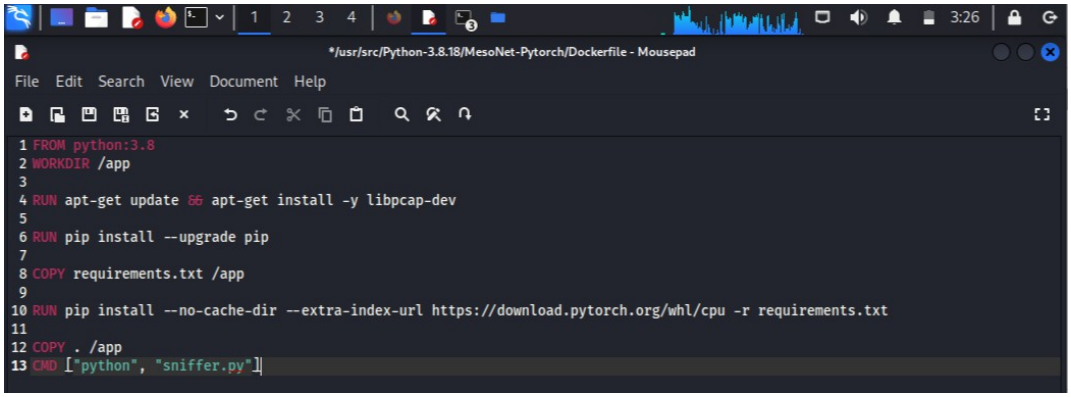


4-Сурет. Жүйенің жалпы құрылымы

Жалған контентті анықтау үшін медиафайлдардағы өте ұсақ бөлшектерді талдай алатын конволюциялық нейрондық желіні қолданатын MesoNet моделі таңдалған болатын. Бұл модельдің басты ерекшелігі - аз есептеу қуатын қамтамасыз етеді және жалған контентті анықтау дәлдігі жоғары.

Қадам 1. Ортаны дайындау. Жүйенің кез келген жерде бірдей және сенімді жұмыс жасауын қамтамасыз ету үшін Docker технологиясы қолданылды.

Практикалық жұмыста барлық қажет кітапханаларды тұрақты түрде қолдану мақсатында dockerfile ресми python:3.8 бейнесіне негізделген болатын. Dockerfile үздік әзірлеу тәжірибелерін ескере отырып жасалған. Мұнда pip-ті жаңарту, барлық қажетті кітапханаларды орнату (requirements.txt), негізгі кодтарды (sniffer.py, deepfake_detector.py және т.б) контейнерге көшіру сияқты кезеңдер жазылған.



5-сурет. Dockerfile құрылымы

Қадам 2. Қажетті құралдар мен кітапханалар тізімі - requirements.txt

Жүйе жұмысын қамтамасыз ету үшін қажетті кітапханалар тізімі жасалған болатын. Requirements.txt тізімі келесі құралдар мен кіта-

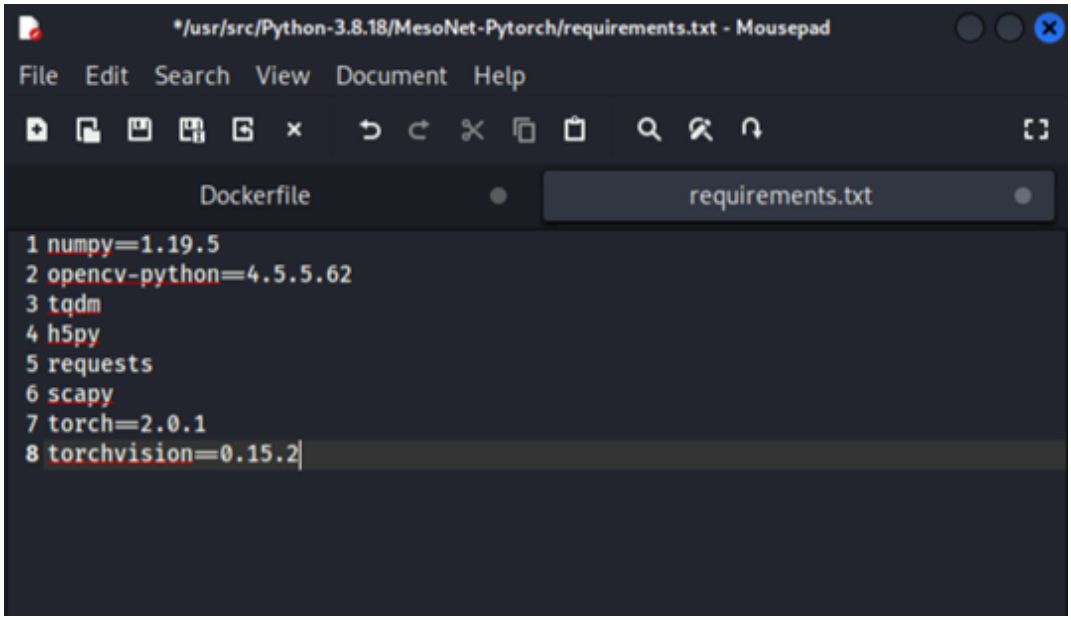
пханаларды қамтиды:

1. Scapy - желілік трафикті талдауға арналған python кітапханасы.

2. PyTorch - терең машиналық оқыту модельдерін құру және жаттықтыруға арналған кітапхана (CPU-есептеулеріне ыңғайлы нұсқасы көрсетілген).

3. Requests - Telegram bot API-мен байланысу үшін.

4. OpenCV - суреттер мен бейнелерді өңдеуге арналған кітапхана.



6-сурет. Requirements.txt мазмұны

Қадам 3. Практикалық іске асыру: негізгі скриптің жұмыс принципі.

Практикалық іске асыру python коды арқылы жүзеге асырылады.

Листинг 1. HTTP трафигін ұстап қалу және толық жауапты жинау

```
from scapy.all import sniff, TCP, Raw, IP
def packet_callback(pkt):
    if not (pkt.haslayer(TCP) and pkt.haslayer(Raw) and pkt.haslayer(IP)):
        return
    ip_layer = pkt[IP]
    tcp_layer = pkt[TCP]
    if tcp_layer.sport != PORT: return
    payload = bytes(pkt[Raw].load)
    conn_key = (ip_layer.src, tcp_layer.sport, ip_layer.dst, tcp_layer.dport)
    if conn_key not in responses:
        if payload.startswith(b"HTTP/1.") and b" 200 " in payload[:15]:
            responses[conn_key] = payload
    else:
        responses[conn_key] += payload
        buf = responses[conn_key]
        if b"\r\n\r\n" in buf:
            head_end = buf.find(b"\r\n\r\n")
            headers_raw = buf[:head_end]
```

```
            for line in headers_raw.decode("latin-1").split("\r\n"):
                if line.lower().startswith("content-length:"):
                    content_length = int(line.split(":",1)[1].strip())
                    break
            body_size = len(buf) - (head_end+4)
            if content_length and body_size >= content_length:
                process_full_response(buf, conn_key)
```

Бұл код бөлігі HTTP жауаптарын толық жинауға арналған. Ол әрбір TCP пакетін өңдеп, жауаптың толық денесін жинайды.

Листинг 2. Суретті сақтап, дипфейкке тексеру

```
def save_and_analyze_image(data_bytes: bytes, content_type: str):
    ext = ".jpg" if "jpeg" in content_type else ".png"
    filename = f"sniffed_{file_counter}{ext}"
    file_path = os.path.join(SAVE_DIR, filename)
    with open(file_path, "wb") as f:
        f.write(data_bytes)

    is_fake = deepfake_detector.is_deepfake(file_path)
    if is_fake:
        notify_telegram(f"Deepfake detected in file: {filename}")
```

Бұл функция екі маңызды істі атқарады. Бірінші ден, суретті жеке файл ретінде сақтайды. Екінші ден, сақталған суретті deepfake_detector модулі арқылы тексереді. Сурет дипфейк деп таңылған жағдайда, Telegram арқылы хабар жіберіледі.

Листинг 3. MesoNet моделы

```
def is_deepfake(image_path):
    image = Image.open(image_path).convert('RGB')
    image = mesonet_data_transforms['val'](image)
    image = image.unsqueeze(0).to(device)
    with torch.no_grad():
        output = model(image)
    _, pred = torch.max(output.data, 1)
    return pred.item() == 1
```

MesoNet моделі медиафайлды дипфейк деп анықтаған жағдайда true мәнін қайтарады [10].

Листинг 4. Telegram арқылы хабарлама жіберу

```
def notify_telegram(message: str):
    url = f"https://api.telegram.org/bot{TELEGRAM_TOKEN}/sendMessage"
    requests.post(
        url,
        data={
            "chat_id": TELEGRAM_CHAT_ID,
            "text": message
        },
        timeout=5
    )
```

Қадам 4. Docker контейнерін іске қосу

Жасалған сниффердi docker ішінде қосу үшін желіге толық қолжетімділік беру қажет. Сондықтан --network=host және --cap-add=NET_ADMIN опцияларын қолданамыз. Бұл Scapy-ге http трафигін ешқандай кедергісіз өңдеуге мүмкіндік береді.

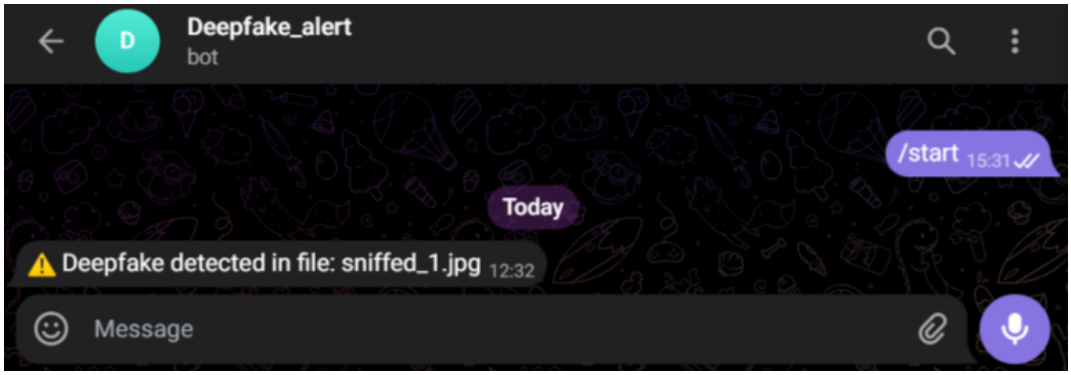
```
┌──(kali㉿kali)-[~]
└─$ sudo docker run --network=host --cap-add=NET_ADMIN http-sniffer

2025-03-18 07:32:23,937 [INFO] [*] Starting sniffer on iface='lo', port=8080
2025-03-18 07:32:31,870 [INFO] [NEW] Http200 from ('127.0.0.1', 8080, '127.0.0.1', 38726)
2025-03-18 07:32:31,877 [INFO] [COMPLETE] ('127.0.0.1', 8080, '127.0.0.1', 38726), body_size=5762, content_length=5574
2025-03-18 07:32:31,878 [INFO] [HEADERS] Content-Type=image/jpeg, Content-Length=5574
2025-03-18 07:32:31,879 [INFO] [INFO] We have 5574 bytes in body, expected 5574
2025-03-18 07:32:31,880 [INFO] [+] Saved 5574 bytes to /tmp/sniffed_1.jpg
/usr/local/lib/python3.8/site-packages/torch/nn/functional.py:1331: UserWarning: dropout2d: Received a 2-D input to dropout2d,
 which is deprecated and will result in an error in a future release. To retain the behavior and silence this warning, please
use dropout instead. Note that dropout2d exists to provide channel-wise dropout on inputs with 2 spatial dimensions, a channel
 dimension, and an optional batch dimension (i.e. 3D or 4D inputs).
  warnings.warn(warn_msg)
2025-03-18 07:32:32,161 [INFO] [Deepfake] result for sniffed_1.jpg: True
2025-03-18 07:32:32,176 [DEBUG] Starting new HTTPS connection (1): api.telegram.org:443
2025-03-18 07:32:32,620 [DEBUG] https://api.telegram.org:443 "POST /bot7794837166:AAGQBl72rKX04w1-QRknnqJjpz_H2TcxJHM/sendMess
age HTTP/11" 200 297
2025-03-18 07:32:32,620 [INFO] [Telegram] Notification sent.
```

7-сурет. Контейнерді желіге қосу конфигурациясы

Қадам 5. Дипфейк анықталған кезде Telegram арқылы хабарлама жіберу

Дипфейк анықталған кезде жүйе автоматты түрде Telegram боты арқылы хабарлама жіберді. Бұл механизм бізге қауіп-қатерге мүмкіндігінше тез жауап беруге және шешім қабылдауға мүмкіндік берді.



8-сурет. Телеграм хабарламасы

Эксперимент нәтижелері біз таңдаған әдістің тиімділігін толық растады: трафикті ұстап қалудан бастап хабарлама жіберуге дейінгі барлық қадамдар қатесіз және жылдам орындалды.

Қорытынды. Бұл зерттеу жұмысы қойылған мақсаттарға жетіп, жалған ақпаратпен күресте өз үлесін қосуға және ақпараттық қауіпсіздікті қамтамасыз етуде тиімді қолдана алатынын көрсетті. Scapy, PyTorch, Docker технологияларын қолдану арқасында желілік трафикті талдап, жасанды контентті тауып алуға арналған автоматтандырылған кешенді жүйе құрылды. Жоба әзірге тек http трафигімен ғана шектелгенімен, болашақта басқа хаттамалармен де интеграцияланады және талдау дәлдігін арттырады деп үміттенеміз. Жасанды интеллектпен машиналық оқытудың алдағы жетістіктері бұл шешімнің тиімділігін арттырып, әртүрлі салаларда қолданылуына мүмкіндік береді. Зерттеу жұмысының барысында құрылған жүйе болашақта SOC және CERT сияқты құрылымдарда пайдалануға бейімделген. Алдағы зерттеулер желілік

трафикті тереңірек талдауды, шифрланған протоколдармен жұмыс істеуді қамтамасыз етуі керек. Бұл бағыттағы зерттеу жұмыстарының арқасында дезинформациямен күресте жаңа деңгейге шығуға мүмкіндік пайда болады.

Әдебиеттер

1. Abbasi M., Shahraki A., Taherkordi A. Deep learning for network traffic monitoring and analysis (NTMA): A survey// Computer Communications. -2021. -Vol.170. -P.19-41. DOI 10.1016/j.comcom.2021.01.021.

2. Bayat N., Jackson W., Liu D. Deep learning for network traffic classification// arXiv preprint. -2021. -No. arXiv:2106.12693. DOI: 10.48550/arXiv.2106.12693.

3. Alanazi S., Asif S. Exploring deepfake technology: creation, consequences and countermeasures// Human-Intelligent Systems Integration. -2024. -Vol.6.-P.49–60. DOI 10.1007/s42454-024-00054-8.

4. Shen Y., et al. Fake news detection on social networks: a survey // Applied Sciences. -2023. -Vol.13(21): 11877. DOI 10.3390/app132111877.

5. Sattarov O., Choi J. Detection of rumors and their sources in social networks: a comprehensive survey// IEEE Transactions on Big Data.-2024.-Vol.11(3) DOI 10.1109/TBDATA.2024.3522801.

6. Gambín Á. F., Yazidi A., Vasilakos A., et al. Deepfakes: current and future trends// Artificial Intelligence Review. -2024. -Vol.57:64. DOI 10.1007/s10462-023-10679-x.

7. Meel P., Raj C., Bhawna. A review of web infodemic analysis and detection trends across multi-modalities using deep neural network // International Journal of Data Science and Analytics. -2025. -Vol. 20(5). -P.4149–4176. DOI 10.1007/s41060-025-00727-w.

8. Zannettou S., et al. The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans// Journal of Data and Information Quality (JDIQ). -2019. -Vol.11(3). -P.1-37. DOI 10.1145/3309699.

9. Alwhbi I. A., Zou C. C., Alharbi R. N. Encrypted network traffic analysis and classification utilizing machine learning// Sensors. -2024. -Vol.24(11): 3509. DOI 10.3390/s24113509.

10. Liu Honggu. MesoNet-Pytorch. -2019. URL: https://github.com/HongguLiu/MesoNet-Pytorch/tree/master. -Қаралған күні: 19.09.2025.

References

1. Abbasi M., Shahraki A., Taherkordi A. Deep learning for network traffic monitoring and analysis (NTMA): A survey// Computer Communications. -2021. -Vol.170. -P.19-41. DOI 10.1016/j.comcom.2021.01.021.

2. Bayat N., Jackson W., Liu D. Deep learning for network traffic classification// arXiv preprint. -2021. -No. arXiv:2106.12693. DOI 10.48550/arXiv.2106.12693.

3. Alanazi S., Asif S. Exploring deepfake technology: creation, consequences and countermeasures// Human-Intelligent Systems Integration. -2024. -Vol.6.-P.49-60. DOI 10.1007/s42454-024-00054-8.

4. Shen Y., et al. Fake news detection on social networks: a survey // Applied Sciences. -2023. -Vol.13(21):11877. DOI 10.3390/app132111877.

5. Sattarov O., Choi J. Detection of rumors and their sources in social networks: a comprehensive survey// IEEE Transactions on Big Data -2024.-Vol.11(3) DOI 10.1109/TBDATA.2024.3522801.

6. Gambín Á. F., Yazidi A., Vasilakos A., et al. Deepfakes: current and future trends// Artificial Intelligence Review. -2024. -Vol.57: 64. DOI 10.1007/s10462-023-10679-x.

7. Meel P., Raj C., Bhawna. A review of web infodemic analysis and detection trends across multi-modalities using deep neural network // International Journal of Data Science and Analytics. -2025. -Vol. 20(5). -P.4149-4176. DOI 10.1007/s41060-025-00727-w.

8. Zannettou S., et al. The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans// Journal of Data and Information Quality (JDIQ). -2019. -Vol.11(3). -P.1-37. DOI 10.1145/3309699.

9. Alwhbi I. A., Zou C. C., Alharbi R. N. Encrypted network traffic analysis and classification utilizing machine learning// Sensors. -2024. -Vol.24(11): 3509. DOI 10.3390/s24113509.

10. Liu Honggu. MesoNet-Pytorch. -2019. URL: https://github.com/HongguLiu/MesoNet-Pytorch/tree/master. -Қаралған күні: 19.09.2025.

Авторлар туралы мәлімет

Сарсембаева З. - магистрант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, e-mail: 040203650680@enu.kz;

Аймичева Г. - PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, e-mail: aimicheva_gi_1@enu.kz;

Назырова А. - PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті,Астана, Қазақстан, e-mail: nazyrova_aye_1@enu.kz.

Information about the authors

Sarsembayeva Z.– Master’s student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, e-mail: 040203650680@enu.kz;

Aimicheva G. - PhD, senior, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, e-mail: aimicheva_gi_1@enu.kz;

Nazyrova A. - PhD, senior lecturer , L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, e-mail: nazyrova_aye_1@enu.kz.