DOI 10.31891/2307-5732-2024-341-5-64
УДК 004.7

ФЕДЧУК ТАРАС
Національний університет «Львівська політехніка»
https://orcid.org/0009-0003-5996-6467
e-mail: taras.b.fedchuk@lpnu.ua
КОРОБЕЙНІКОВА ТЕТЯНА
Національний університет «Львівська політехніка»
https://orcid.org/0000-0003-2487-8742
e-mail: tetianakorobeinikova@gmail.com

ГІБРИДНИЙ МЕТОД АНАЛІЗУ ТА ІДЕНТИФІКАЦІЇ ШКІДЛИВОГО DoH-ТРАФІКУ

У роботі розглядаються новітні підходи, методи і засоби для розробки системи ідентифікації DoH-трафіку, яка на відміну від аналогів, базується на гібридному підході до ідентифікації шкідливого трафіку: із застосуванням відкритих інструментів визначення зашифрованого DNS-трафіку та спеціалізованих моделей машинного навчання. Гібридний підхід передбачає попередню обробку даних, балансування класів та застосування перехресної перевірки для забезпечення точних і неупереджених результатів. Результати цього дослідження можуть бути застосовані в організаціях, освітніх установах, компаніях і урядових установах для своєчасного виявлення шкідливого типу DoH-трафіку.

Ключові слова: кібербезпека, безпека в DNS, DNS over HTTPS, DoH-трафік, гібридний підхід, шкідливий трафік.

FEDCHUK TARAS, KOROBEINIKOVA TETIANA
Lviv National Technical University

HYBRID METHOD FOR ANALYSIS AND IDENTIFICATION OF MALICIOUS DOH-TRAFFIC

This study addresses the challenges associated with detecting DNS over HTTPS (DoH) traffic, a relatively new protocol that has not been extensively researched. The detection methods discussed include TLS inspection, application logging, and open-source tools such as Zeek and RITA. TLS inspection, which involves decrypting and analyzing traffic, is the most intrusive and requires full control over the network and client configurations. Application logging, such as that available in Mozilla Firefox, necessitates administrative control over client systems, which may be impractical. Zeek analyzes network logs to identify domains accessed without regular DNS queries, while JA3 fingerprints and RITA focus on detecting malicious DoH traffic by analyzing TLS handshake parameters and beacon-like activities, respectively. Additionally, maintaining up-to-date blacklists of IP addresses and SNI values can help identify DoH traffic but faces scalability and evasion challenges. The study highlights that no current solution is entirely feasible, with many requiring excessive administrative overhead or failing to scale effectively. A hybrid approach using machine learning models and traffic analysis, as illustrated by the CIRA-CIC-DoHBrw-2020 dataset, is proposed for more effective detection of malicious DoH traffic. This approach involves the architecture of a two-stage DoH traffic identification system is presented, consisting of three subsystems: traffic, training and evaluation, and identification. They operate sequentially, with the system's function being traffic identification, training, testing, and information processing within the DoH protocol. The next step is process of cross-validation, which involves training a machine learning model K times, with each iteration using a different fold as the validation set, while the remaining folds serve as the training set.

***The aim of this work:** Development and implementation a DoH traffic identification system, which, unlike existing solutions, is based on a hybrid approach to identifying malicious traffic using open tools for detecting encrypted DNS traffic and specialized machine learning models.*

Keywords: cybersecurity, DNS security, DNS over HTTPS, DoH traffic, hybrid approach, malicious traffic.

Постановка проблеми

Комплекс проблем і завдань в галузі ідентифікації трафіку є дуже важливою в кібербезпеці і є фундаментальною у функціонуванні SIEM-систем, фаєрволів нового покоління, різного роду інструментів, що здійснюють інспекцію над трафіком, системами IDS/IPS та іншими комерційними продуктами, які надають послуги SOC чи MSSP для корпорацій [1, 2]. Дана задача розглядається на різних рівнях детектування трафіку з подальшою затримкою для детального аналізу, блокування або пропускання потоку даних, вона вирішується при виявленні 0-day атаки, попередженні різного роду експлойтів, троянів та інших не менш небезпечних атак [3, 4]. Важливо вчасно ідентифікувати тип трафіку, превентивно надати йому оцінку і здійснити конкретну дію з подальшим проходженням даних через канал зв'язку до отримувача, щоб забезпечити цілісність та конфіденційність даних [5].

Зокрема, важливим напрямком сучасних досліджень в галузі кібербезпеки є вирішення задачі ідентифікації шкідливого DoH-трафіку [6, 7], оскільки в сучасному світі під час відображення імен для інтернет-ресурсів все частіше працюють DoH-ресолвери, що приховують відкритий DNS-трафік, використовуючи протокол HTTPs, і таким чином дають можливість зловмисникам приховати свої дії та нанести шкоду в інформаційному просторі.

У даній науковій роботі було запропоновано гібридний метод вирішення задачі ідентифікації шкідливого DoH-трафіку, який є ефективнішим у порівнянні із традиційними інструментами та аналізаторами даних. Запропонований метод може бути корисний для вирішення задач, пов'язаних з аналізом шифрованого трафіку та під час розробки нових методів машинного навчання для протоколу DNS.

Основна увага наукового дослідження спрямована на розробку гібридного методу ідентифікації шкідливого DoH-трафіку. На відміну від аналогів (традиційних аналізаторів та інструментів виявлення і розпізнавання трафіку), запропонований нами метод має перевагу за рахунок застосування відкритих інструментів визначення зашифрованого DNS-трафіку та спеціалізованих моделей машинного навчання. Це дає можливість здійснити якісний аналіз DoH-трафіку та досягти вищої результативності під час роботі із

шифрованими даними.

В статті розглянуті ключові виклики, пов'язані з виявленням DoH-трафіку. Зокрема, виявлено, що зазвичай методи ідентифікації шкідливого трафіку передбачають інспекцію TLS, ведення журналів додатків та використання рішень на зразок Zeek і RITA. Також відомо, що інспекція TLS, яка передбачає розшифрування та аналіз трафіку, є найбільш інвазивною, тож вимагає повного контролю над конфігураціями мережі та клієнтів. Виявлені ці та інші недоліки спонукають шукати нові рішення в цьому напрямку, тож існує потреба у розробці нових підходів, методів та засобів ідентифікації шкідливого DoH-трафіку.

Аналіз останніх досліджень

Питаннями, пов'язаними ідентифікації шкідливого DoH-трафіку займаються такі відомі сучасні вчені, як А. А.-Хайджа, К., Алохалі, М, Одех, А. в напрямку виявлення зловмисного DoH-трафіку за допомогою гібридного підходу («A Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach») [8]; Абу Аль-Хайджа, Q., Аль-Бадаві, А. щодо маршрутизації мережевого трафіку Інтернету речей з можливістю атак із використанням машинного навчання («Attack-Aware IoT Network Traffic Routing Leveraging Ensemble Learning») [9]; Сінгх, С.К. та Рой, П.К. в напрямку виявлення зловмисного DNS через https-трафік за допомогою машинного навчання («Detecting malicious dns over https traffic using machine learning») [10], Вазен М. Шбеїр, Зибальт Хлоз, Ентоні Гухот та Ізабель Крісмен в напрямку обходу фільтрації HTTPS на основі SNI («Efficiently bypassing SNI-based HTTPS filtering») [11], Карел Хайнек, Дмитрій Векшин, Ян Люксембурк, Томаш Чейка і Армін Васічек розвивали думки про зловживання DNS через HTTPS [12] та ін.

Амар Одех у своїй роботі [8] розглядає два рівні ідентифікації DoH-трафіку для досягнення показників точності у 99.4%, а Ахмед Аль-Бадаві у роботі [9] базується на вивченні методів навчання під наглядом для оцінки розробленої NIDS (система виявлень вторгнень у мережу); в той же час Сінгх, С.К. та Рой, П.К. у роботі [10] пішли шляхом використання класифікаторів машинного навчання для виявлення зловмисної активності на рівні DNS у середовищі DoH. Дмитро Векшин у [12] описує три реальні сценарії зловживань у веб-середовищі. Проте всі вони єдині у тому, що на даний момент не існує традиційних засобів чи методів для ефективної ідентифікації та аналізу шифрованого DoH-трафіку і для максимальної результативності потрібно використовувати методи машинного навчання, які в поєднанні із уже розробленими аналізаторами та класифікаторами формують гібридний підхід для вирішення основної задачі.

Це дає авторам можливість розвинути напрямок гібридного підходу до ідентифікації шкідливого DoH-трафіку. Оскільки існує протиріччя між необхідністю імплементації інструментів машинного навчання і недостатнім рівнем наявного науково-методичного апарату, пропонується наукове дослідження гібридних методів ідентифікації шкідливого DoH-трафіку [6, 7].

За останні десять років було впроваджено багато протоколів, які мають потужний вплив на інтернет з точки зору кібербезпеки та захисту даних. Одним з таких є DNS over HTTPS (DoH). DoH – це протокол прикладного рівня, який працює за класичною схемою запит-відповідь, із урахуванням відмінностей між версіями протоколу HTTP. Даний протокол став революційним з точки зору функціонування DNS після успішного запуску найбільш популярними web-браузерами (Firefox, Google Chrome, Safari) і через свою специфіку роботи на мережевому рівні, DoH виглядає як типова HTTPS-комунікація. Він встановлює з'єднання по порту tcp/443, виконує TLS handshake та передає зашифровані дані. Це дозволяє аналізувати вміст DNS-запитів та використовувати додатковий захист, проте даний протокол приніс багато неоднозначностей, а саме, його складно розпізнати, адже він схожий до звичайної HTTPS-комунікації і ще складніше розпізнати шифровані дані на предмет шкідливості з боку адміністрування та безпеки даних [6]. У статті [6]основна увага приділяється ідентифікації DoH-трафіку та методів його розпізнавання з використанням відкритих інструментів.

Постановка задачі

Метою роботи є: розробка та впровадження системи ідентифікації DoH-трафіку, яка на відміну від аналогів, базується на гібридному підході до ідентифікації шкідливого трафіку із застосуванням відкритих інструментів визначення зашифрованого DNS-трафіку та спеціалізованих моделей машинного навчання.

Основа для дослідження

Наше наукове дослідження базується на тому, що DoH-трафік займає чільне місце в сучасних інформаційних технологіях, зокрема передавання даних і може бути вразливістю з точки зору кібербезпеки та захисту інформації, тому його ідентифікація є важливим завданням, а ідентифікація шкідливого DoH-трафіку є ще складнішим і набагато важливішим завданням. Це дасть можливість ефективно справлятися з потоком даних, регулювати його та впливати на подальший рух, захищати персональні дані, викривати зловмисні дії і опирається на традиційних засобах ідентифікації та аналізу трафіку, а також сучасних методів машинного навчання.

Відомо, що на мережевому рівні моделі взаємодії відкритих систем [1, 2], DoH працює за принципом HTTPS-комунікації [3]. Це означає, що встановлюється з'єднання через порт TCP/443 [4], виконується TLS-handshake [3] і передаються зашифровані дані [5]. Цей механізм із залученням протоколу HTTPS, шифрує DNS-трафік, ускладнюючи аналіз вмісту самих DNS-запитів та забезпечує їх додатковий захист [1]. Зазвичай системи, що використовують аналіз DNS-даних, блокують доступ до певних веб-ресурсів шляхом вибіркового блокування DNS-запитів [13]. Однак, правильна ідентифікація DoH є складною задачею, що може бути вирішена шляхом застосування спеціалізованих моделей машинного навчання.

За останній період часу було проведено багато досліджень по інтенсивності використання трафіку DoH. Загалом з'явився науковий інтерес до теми «DNS resolving у кібербезпеці», та все ж є ще багато тем, які були малодосліджені або не досліджені взагалі.

Амар Одех розглядає два рівні ідентифікації DoH-трафіку, використовуючи методи Random Forest, Adaboost trees, принциповий компонентний аналіз та підхід Random Under-sampling для досягнення показників точності ідентифікації DoH-трафіку у 99.4%, а Ахмед Аль-Бадаві базується на вивченні шести методів навчання під наглядом, які належать до трьох різних класів:

- ансамблеві методи;
- методи нейронної мережі;
- методи ядра для оцінки розробленої NIDS (система виявлень вторгнень у мережу).

Під час дослідження вони використовують набори даних distilled-Kitsune-2018 і NSL-KDD.

Група науковців у складі Сінгх, С.К. та Рой, П.К. пішли шляхом використання класифікаторів машинного навчання, таких як:

- наївний базис (NB);
- логістична регресія (LR);
- випадковий ліс (RF);
- K-найближчий сусід (KNN);
- градієнт підвищення (GB) для виявлення зловмисної активності на рівні DNS у середовищі DoH.

Експерименти проводились на еталонному наборі даних MO3 (CIRA-CIC-DoHBrw-2020). Водночас Дмитро Векшин вважає, що можна описати три реальні сценарії зловживань у веб-середовищі, які демонструють, як постачальники інтернет-послуг можуть вберегти клієнтів від небезпечного DoH-трафіку, використовуючи блокування, перенаправлення та розподілені DoH-тригери. Науковці Вазен М. Шбеїр, Зибальт Хлоз, Ентоні Гухот та Ізабель Крісмен розглядають найновіші техніки фільтрації трафіку HTTPS. Одна з них базується на полі індикації імені сервера (SNI) TLS і яка нещодавно реалізована в багатьох рішеннях брандмауера. Їх головний внесок – це оцінка надійності цього розширення SNI для належної ідентифікації та фільтрації трафіку HTTPS. Вони показують, що SNI має дві слабкості, щодо:

- зворотної сумісності;
- кількох служб, які використовують один сертифікат.

Завдяки плагіну веб-переглядача під назвою «Escape», який науковці розробили та впровадили, вони демонструють, як ці недоліки можна практично використати для обходу брандмауерів і систем моніторингу, що покладаються на SNI. Результати показують позитивну оцінку (правила брандмауера успішно обходяться) для всіх перевірених веб-сайтів.

Проведений аналіз останніх наукових праць та актуальних джерел технічної інформації дає підґрунтя для детального вивчення протоколу DoH та способу ідентифікації шкідливого DoH-трафіку. З точки зору інформаційної безпеки завдання можна розділити на дві категорії:

- виявлення присутності DoH в мережі;
- ідентифікації шкідливого DoH-трафіку.

Методи та засоби ідентифікації шкідливого DoH-трафіку

Для розпізнавання DNS over HTTPS трафіку було проведено відносно небагато досліджень. Це пояснюється тим фактом, що DoH є новим протоколом, і рішення не виглядають достатньо тривіальними для реалізації за допомогою базової евристики [3].

Метод перевірки TLS – це найбільш інвазивний метод ідентифікації DoH-трафіку, оскільки він вимагає повного розшифрування трафіку та його перевірки, щоб дізнатися, які мережеві потоки передають DNS-дані. Основне налаштування полягало б у встановленні проміжного блоку, який би розшифровував і перевіряв трафік для виявлення. Рис. 1 ілюструє цю конфігурацію в простому вигляді.

Дешифрування TLS вимагає технічного і бюрократичного контролю над мережею, оскільки весь трафік буде перевірятися. Швидше за все, це також вимагає контролю над залученими клієнтами всередині мережі: оскільки встановлюється TLS-проміжний блок, клієнти повинні прийняти його як дійсну кінцеву точку, оскільки його ім'я хоста не співпаде з тим, до якого клієнти намагаються отримати доступ. Або клієнти змушені прийняти TLS-сертифікат проміжного блоку вручну (зазвичай через параметр, наданий веб-браузерами), або новий сертифікат потрібно додати як надійний на клієнтській машині. Навіть у цьому випадку це не вирішить проблеми із закріпленими сертифікатами [14]. Використовуючи цей механізм, клієнтська програма об'єднується з певними сертифікатами довірених центрів і очікує знайти ці центри в ланцюжку перевірки.

Якщо використовуються закріплені сертифікати, з'єднання не встановлюється, оскільки, навіть якщо сертифікат проміжного блоку є надійним, він не відповідатиме очікуванням програми. Загалом, ця техніка можлива лише за певних умов, таких як повний контроль над мережею та бажання клієнтів повністю розшифрувати та перевірити свій трафік.

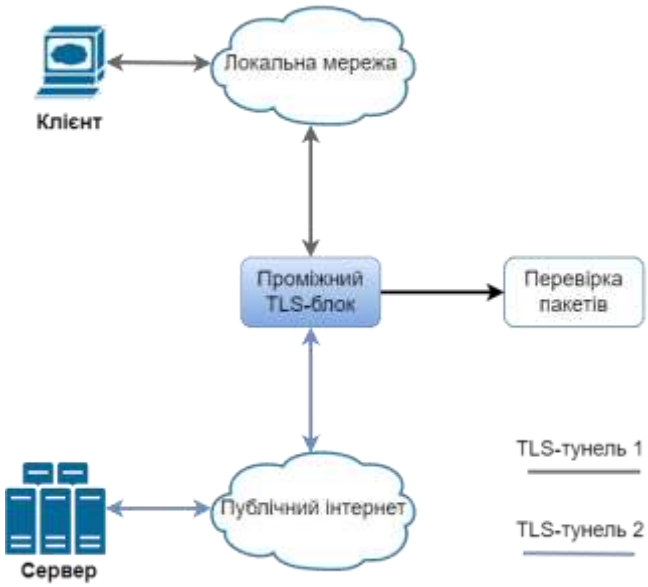

Рис.1. Конфігурація перевірки TLS

Метод логування програми. Браузер Mozilla Firefox, наприклад, пропонує можливість реєструвати кожен DNS-запит (зашифрований чи ні) [15]. Як і в попередньому варіанті, тут потрібен адміністративний контроль над клієнтом, який виконує запити, що може бути неможливим. Персональні мобільні пристрої та ноутбуки складніше або неможливо контролювати таким чином, і навіть тоді кожен окремий клієнт у мережі має запустити програму, яка може реєструвати запити DNS, і кожен із них має бути налаштований. Загалом ця техніка потребує великої кількості роботи адміністратора для встановлення та підтримки.

Засоби для аналізу мережевого трафіку з відкритим кодом. Одним з таких інструментів є Zeek [16]. Zeek – це інструмент аналізу мережі та моніторингу безпеки з відкритим кодом. Його робота полягає в аналізі Zeek-логів для виявлення відвіданих сайтів, для яких не було регулярних запитів DNS. Це створює дві проблеми: 1) складність ідентифікації відвіданих сайтів під час HTTPS-шифрування, і 2) той факт, що фактичні з'єднання DoH досі не ідентифіковано, навіть якщо його наявність можна підтвердити. Для цього пропонується використання **аналізу відбитків пальців** JA3 [17]. Цей тип відбитків працює через обчислення хеш-рядка з використанням параметрів, які спостерігаються під час рукостискання TLS. Цей підхід корисний при роботі з кампаніями зловмисного ПЗ. Основна ідея полягає в тому, щоб заблокувати командні та контрольні сервери з електронними відбитками, аби зловмисне ПЗ не могло підключитися до них і отримати інструкції. Зазвичай ці сервери зберігаються статичними, оскільки зловмисне ПЗ має знаходити їх автономно, але сервери DoH можуть не підтримуватися клієнтом. Користувач може перейти на новий DoH-ресолвер або може просто використати HTTPS проксі-сервер.

Іншим інструментом для аналізу мережевого трафіку є RITA (Real Intelligence Threat Analytics) [17]. Цей інструмент використовує Zeek-логи для **виявлення активності «маяків»** серед іншого підозрілого трафіку. Незважаючи на те, що RITA може позначати з'єднання DoH як «маячкову активність», кількісні показники щодо точності чи помилкових спрацьовувань не наводяться. Тести складаються з сеансу веб-перегляду тривалістю 5 хвилин, що менше, ніж очікується від звичайного користувача. Активність маяків визначається постійним часом між пакетами протягом часу та постійними розмірами пакетів протягом часу. Таким чином, можна поставити питання про те, чи з'єднання DoH все ще мають характеристики, подібні до маяків, протягом тривалих періодів часу. Тим не менш, результат, наданий для RITA, є цікавим, оскільки він вказує на характеристики DoH-трафіку, принаймні в часовому масштабі експерименту.

Аналізуючи вихідний код інструменту, RITA вважає такими характеристиками, як маяки, зокрема: малі розміри пакетів, низька нерівність розмірів пакетів, низька дисперсія в часі між пакетами (постійна пропускна здатність).

Методи збереження оновлених чорних списків IP-адрес та значень SNI. Крім запропонованих методів у дослідженні [16], є ще два підходи, які можна застосувати для виявлення DoH-трафіку. Обидва вони полягають у збереженні оновлених чорних списків як IP-адрес, так і значень SNI (Server Name Indication) [19]. Для IP-адрес було б раціонально скласти список відомих DoH-ресолверів і контролювати підключення до них. Хоча це може бути дуже простим для реалізації підходом, зараз існує понад 40 відомих ресолверів [20], і варто очікувати, що ця кількість з часом зросте, враховуючи те, наскільки новий протокол і нещодавнє впровадження основними браузерами, тому це рішення має масштабуватися з часом. Варто зазначити, що тривіальний HTTPS-проксі може перевершити цей підхід. Що стосується значення SNI, то це розширення TLS, яке вказує ім'я хоста, до якого клієнт намагається підключитися, тому, коли значення SNI надсилається незашифрованим, відбувається витік інформації про зв'язок. Таким чином, надісланий рядок може бути використаний для створення чорного списку DoH-ресолверів. Окрім тієї ж проблеми, що й з IP-адресами, де необхідно підтримувати оновлену базу даних, виникають інші проблеми, такі як можлива відсутність цього поля або його

шифрування, як це нещодавно було запропоновано в [21]. Навіть за його наявності, модифікація цього поля для шкідливих цілей вже є сучасною технікою [11]. Загалом, жодне з попередніх рішень не здається життєздатним, повним чи достатньо зрозумілим.

Індикатори зловмисної діяльності

Отже, метод перевірки TLS і метод логування додатків, передбачають порушення конфіденційності користувача та надмірний адміністративний контроль, який може бути неможливим через технічні чи бюрократичні причини. З іншого боку, цифрові відбитки сервера, збір IP-адрес і моніторинг SNI є релевантними рішеннями нової проблеми, які, як видається, не будуть масштабуватися в довгостроковій перспективі. Крім того, їх можна легко обійти за допомогою HTTPS-проксі, які зручно працюють з DoH-трафіком. Запропоновані більш концептуальні рішення для аналізу трафіку за допомогою Zeek і RITA, проте в них не надано кількісних показників для збору інформації. Шкідливий DoH-трафік складно ідентифікувати, оскільки він розроблений так, що виглядає як звичайний HTTPS-трафік [10]. На рисунку 2 показано кілька індикаторів, які можуть свідчити про зловмисну діяльність.

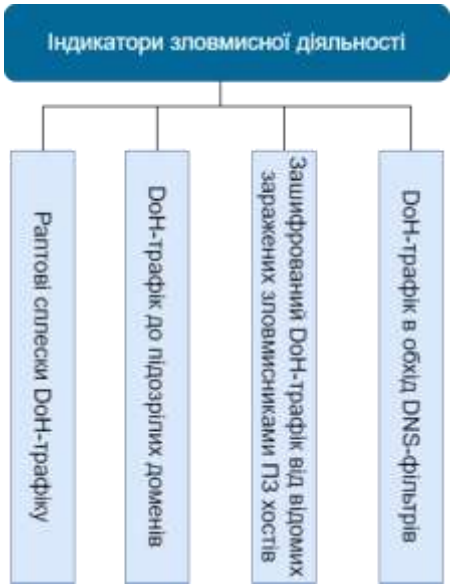

Рис.2. Індикатори зловмисної діяльності

Індикаторами шкідливої діяльності є:

1) Раптові сплески трафіку DoH: раптове збільшення мережевого трафіку може вказувати на те, що зловмисники використовують DoH для обходу фільтрів DNS [8].
2) DoH-трафік до підозрілих доменів: Якщо велика кількість DoH-трафіку надходить до відомих доменів, які пов'язані зі зловмисним програмним забезпеченням, фішингом або іншими видами зловмисної діяльності, це може бути ознакою того, що зловмисники використовують DoH для доступу до цих доменів [8].
3) Зашифрований DoH-трафік від відомих заражених зловмисним програмним забезпеченням хостів: якщо відомо, що хости в мережі інфіковані зловмисним ПЗ, і зашифрований трафік DoH надходить із цих хостів, це може означати, що зловмисне ПЗ використовує DoH для зв'язку зі своєю командою і сервери керування [22].
4) Трафік DoH в обхід DNS-фільтрів: якщо реалізовані DNS-фільтри блокують доступ до відомих шкідливих сайтів і DoH-трафік обходить ці фільтри, це може означати, що хтось використовує DoH для обходу реалізованих DNS-фільтрів.

Щоб виявити зловмисний трафік DoH, системі може знадобитися реалізація спеціальних інструментів і методів, таких як глибока перевірка пакетів, аналіз поведінки або алгоритми машинного навчання. Крім того, важливо бути в курсі останніх загроз і вразливостей, пов'язаних з DoH, і дотримуватися найкращих практик щодо захисту мережі та кінцевих точок [9].

Архітектура двоступеневої системи ідентифікації DoH-трафіку

Рис. 3 ілюструє загальну архітектуру двоступеневої системи для ідентифікації зловмисного DoH-трафіку за допомогою гібридного підходу до навчання даної системи.

Запропонована система складається з трьох складових:

1) підсистема трафіку;
2) підсистема навчання та оцінки;
3) підсистема ідентифікації.

Підсистема трафіку. Ця підсистема передбачає дії з підготовки та попередньої обробки DNS-даних для налаштування інформації для процесу машинного навчання. У цьому дослідженні набір даних CIRA-CIC-DoHBrw-2020 використовувався для оцінки запропонованої моделі ідентифікації зловмисного DoH-трафік (DoH) за допомогою моделей контрольованого навчання.

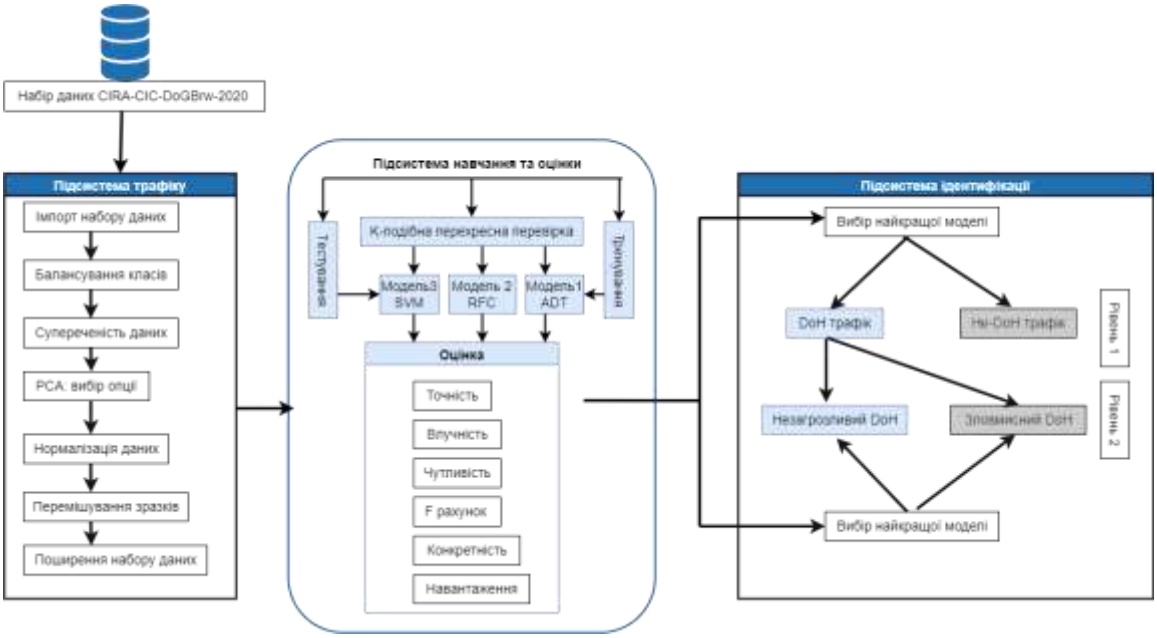

Рис.3. Архітектура двоступеневої системи ідентифікації DoH-трафіку

Набір даних CIRA-CIC-DoHBrw-2020 спочатку складався з двох вибірок: (1)

1) набір даних першого рівня, який використовується для класифікації трафіку DNS на DoH або не-DoH і складається з 269,643 зразків для трафіку DoH і 897,494 зразків для не-DoH Трафік DoH;
2) набір даних другого рівня, який використовується для класифікації трафіку DoH на незагрозливу DoH або шкідливу DoH і складається з 20,000 зразків для безпечного трафіку DoH і 249,836 зразків для зловмисного трафіку DoH.

Підсистема навчання та оцінки. Після попередньої обробки та підготовки даних їх можна передати наступній підсистемі навчання та оцінки. Відповідно до архітектури системи, показаної на рисунку 3, було оцінено дану підсистему з використанням трьох основних потужних підходів до навчання за участі: дерев Adaboost (AD) [23], випадкових тонких дерев (RFC) і машин опорних векторів. (CBM). Щоб оцінити продуктивність кожної моделі, були використані стандартні оціночні метрики машинного навчання (точність, влучність, чутливість, F рахунок, конкретність, навантаження).

Підсистема ідентифікації. Після того, як моделі навчання розроблені, навчені, перевірені та оцінені, вибирається найкраща серед трьох моделей для виконання операції ідентифікації на кожному рівні. Перший рівень перевіряє трафік, щоб ідентифікувати чи це DoH або не-DoH. Якщо трафік належить до DoH, тоді на другому рівні трафік DoH додатково досліджується, щоб визначити його як незагрозливий DoH або зловмисний DoH. Реалізовані моделі навчання були оцінені для кожного рівня окремо.

Робота із даними

Незважаючи на всі наявні механізми безпеки, робота із даними передбачає ідентифікацію, навчання, тестування та обробку інформації в протоколі DoH, де зловмисники все ще можуть використовувати розширені підходи до атак, щоб викрасти інформацію під час передачі зловмисного DoH-трафіку. Тому, як і будь-яка система захисту від атак [9], існує занепокоєння щодо виявлення зловмисного DoH-трафіку за допомогою інтелектуальних контрольованих методів. Попередньо представлена архітектура двоетапної системи для ідентифікації DoH-трафіку, а також шкідливого типу трафіку із застосуванням відкритих інструментів визначення зашифрованого DNS-трафіку та оптимізації даних за допомогою гібридного підходу до навчання демонструє, що така схема є ефективною у нашій задачі.

На рис.4 показано розподіл гістограми для набору даних CIRA-CIC-DoHBrw-2020.

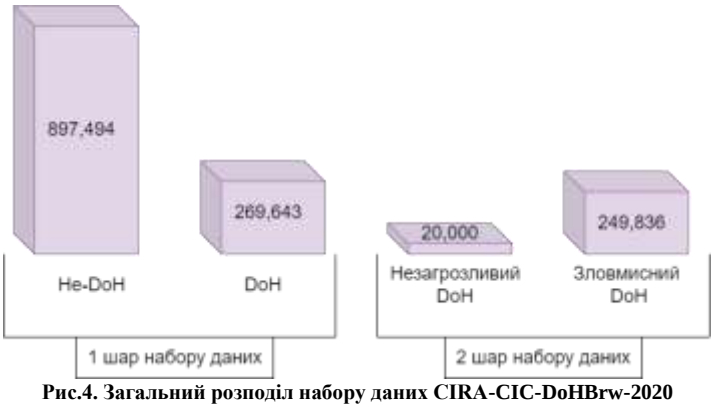

Рис.4. Загальний розподіл набору даних CIRA-CIC-DoHBrw-2020

Зразки DNS-даних були згенеровані в обох наборах даних з використанням 34 ознак і однієї мітки класу. Коли набір даних зібрано та імпортовано за допомогою таблиць MATLAB, він передбачав такі послідовні процеси обробки:

1) балансування класів;
2) перебір даних;
3) вибір функції;
4) нормалізація даних;
5) перемішування зразків;
6) розповсюдження набору даних.

Процес балансування класів: оскільки набір даних CIRA-CIC-DoHBrw-2020 є незбалансованим за класами, був застосований підхід випадкової недостатньої вибірки (random under-sampling – RUS) [24], щоб збалансувати всі класи в наборі даних і мінімізувати кількість зразків в кожному класі. Рис. 5 ілюструє гістограму розподілу для збалансованого скороченого набору даних.

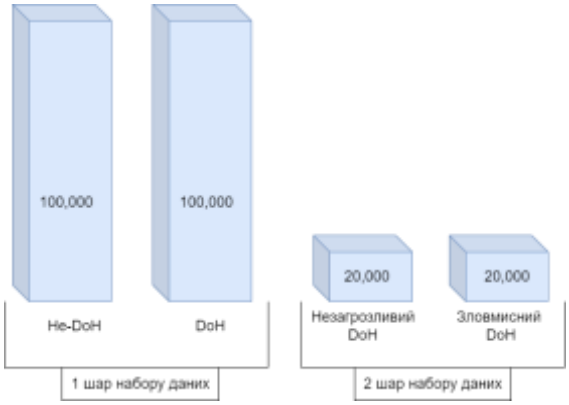

Рис.5. Загальний розподіл набору даних після збалансування та недостатньої вибірки

Процес перебору даних: це процес забезпечення того, що дані безпомилкові та готові до використання іншими навчальними модулями. Під час обробки даних [25] застосовуються кілька дій, включаючи очищення даних від будь-яких шумних або помилково введених записів, усунення дублікатів у вибірках, заповнення відсутніх даних (нульовими, мінімальним, максимальним або середнім значенням) і дослідження даних для перевірки розподіл і частоту (за допомогою гістограми) для кожної цільової мітки.

Процес вибору функції: зменшує кількість вхідних атрибутів, які надаються та обробляються моделлю контрольованого виявлення/класифікації. Це покращує продуктивність моделі за рахунок збільшення швидкості передбачення та мінімізації витрат на прогнозування. У цьому дослідженні ми використовували аналіз головних компонентів (PCA) на етапах попередньої обробки, щоб зменшити розмірність (зменшити кількість вхідних наборів функцій). PCA зменшує кількість вимірів (функцій), одночасно збільшуючи інтерпретацію даних і зберігаючи максимальну кількість інформації. У результаті, щоб задовольнити легку продуктивність запропонованої моделі, було використано найменшу кількість функцій, які максимізують продуктивність системи. Остаточний набір включає лише шість із тридцяти чотирьох функцій (FlowBytesSent, FlowReceivedRate, PacketLengthStandardDeviation, PacketLengthMean, PacketLengthMedian, PacketLengthMode).

Процес нормалізації даних: під час обробки набору даних ми можемо виявити деякі функції зі значеннями, розкиданими в широких масштабах. Це може негативно вплинути на продуктивність/стабільність класифікатора під час процесу навчання. Нормалізація даних використовується для подолання цієї проблеми шляхом перетворення функцій у аналогічний масштаб. Нормалізоване значення x (X_{scaled}) визначається так (1):

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Процес перемішування зразків: передбачає змішування вибірки даних (рядків) із збереженням логічних зв'язків між функціями (стовпцями). Це означає випадкову зміну розташування для кількох зразків, але зберігаючи значення ознак у тому самому порядку. Перетасування має важливе значення для усунення будь-якого порядку сортування в наборі даних, гарантуючи, що класифікатор не переобладнується до певного порядку дуетного сортування класу.

Процес розповсюдження набору даних: передбачає поділ набору даних на набори даних для навчання та тестування (перевірки). У цьому дослідженні ми використали 75% набору даних для навчання, тоді як 25% залишилося для тестування моделі за допомогою п'ятикратної перехресної перевірки для оцінки продуктивності моделі для всіх складок даних у наборі даних. П'ятикратна перехресна перевірка зазвичай використовується для усунення зміщення класифікатора в бік одного з цільових класів під час процесу перевірки [8].

Рис. 6 ілюструє процес п'ятикратної перехресної перевірки. Показники продуктивності розраховуються як середнє значення результатів п'яти експериментів (у п'ять разів).

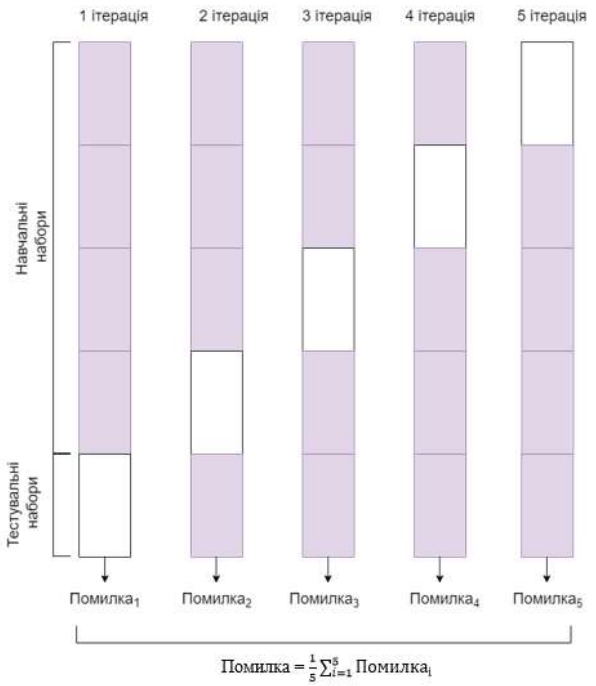

Рис.6. Демонстрація п'ятикратної перехресної перевірки

Отже, в результаті аналізу DNS-даних було розроблено та впроваджено двоетапну систему для ідентифікації DoH-трафіку, а також шкідливого типу трафіку із застосуванням відкритих інструментів визначення зашифрованого DNS-трафіку і це означає, що була здійснена оптимізація даних за допомогою гібридного підходу до навчання системи і така схема виявилась еталонною у нашій роботі.

Були проведені експерименти з розповсюдженням набору даних, використавши 75% набору DNS-даних для навчання, і 25% для тестування моделі за допомогою п’ятикратної перехресної перевірки для оцінки продуктивності моделі для всіх складок даних у наборі даних. Це дозволило забезпечити раціональну, неупереджену та всебічну перевірку DNS-даних. Процес перехресної перевірки передбачає навчання моделі машинного навчання K разів (тобто п’ять разів у нашому випадку), кожен з яких використовує іншу згортку як набір перевірки, а решта згорток – як навчальний набір. Це означає, що кожна точка даних у вихідному наборі даних використовується як для навчання, так і для перевірки принаймні один раз, а також дане співвідношення тестування та тренування системи є найбільш оптимальним для ефективної роботи з аналізом DNS-даних.

Висновки з даного дослідження
і перспективи подальшого розвитку у даному напрямі

Представлена робота використовує гібридний метод ідентифікації шкідливого трафіку із застосуванням відкритих інструментів визначення зашифрованого DNS-трафіку та спеціалізованих моделей машинного навчання у спеціалізованій системі ідентифікації DoH-трафіку обох типів (зловмисного та незагрозливого). Застосування запропонованого гібридного методу ідентифікації шкідливого трафіку поповнює наявний науково-методичний апарату у галузі та розширює арсенал методів та засобів для подальшого дослідження точності та влучності алгоритмів визначення наборів DNS-даних.

Дослідження методів ідентифікації трафіку DNS over HTTPS виявило кілька підходів, проте вони виявилися не достатньо дієвими. Скажімо, перевірка TLS та логування програм є дуже інвазивними методами та потребують значного адміністративного контролю, що може бути технічно або бюрократично складно реалізувати. Інструменти для ідентифікації DoH-трафіку з відкритим кодом, такі як Zeek та RITA, пропонують рішення у вигляді zeek-логів для виявлення активності «маяків», використовують аналіз відбитків пальців JA3, але ці методи також мають обмеження у складності застосування, у точній ідентифікації та можливості обходу. Використання чорних списків IP-адрес і значень SNI є практичними, але також знаходяться під впливом проблем масштабування та можливості обходу через HTTPS-проксі. Загалом, розглянуті авторами існуючі методи та засоби не забезпечують повного рішення для ідентифікації DoH-трафіку, особливо в контексті зловмисного використання. Виявлено, що інтеграція нових підходів, таких як машинне навчання для аналізу трафіку, може забезпечити кращу ідентифікацію зловмисного DoH-трафіку, проте ці рішення потребують постійного вдосконалення і валідації. Важливо продовжувати досліджувати а також вдосконалювати методи та засоби для підвищення точності та ефективності ідентифікації зловмисного DoH-трафіку.

Зокрема, у даній статті виявлено, що відкриті інструменти для ідентифікації DoH-трафіку, перевірка TLS та використання значень SNI не є релевантними методами і самостійно не здатні вирішити задачу ідентифікації шифрованого DNS-трафіку, проте використовуючи методи машинного навчання, можна досягнути кращих результатів. Також було запропоновано двоступеневу систему ідентифікації DoH-трафіку і структуровано та оптимізовано набір DNS-даних, використовуючи п'ятикратну перехресну перевірку.

Література

1. Т.І. Коробейнікова, С.М. Захарченко (2021) Технології захисту локальних мереж на основі обладнання CISCO: навч. Посібник – Львів, Видавництво Львівської політехніки, 188 с.
2. Т.І. Коробейнікова, С.М. Захарченко. (2022) Комп'ютерні мережі: навч. Посібник – Львів, Видавництво Львівської політехніки, 228 с.
3. P. E. Hoffman and P. McManus, Oct. (2018) DNS Queries over HTTPS (DoH), RFC 8484, Tech. Rep. 8484.
4. P. Mockapetris, Domain names - implementation and specification, RFC 1035 (Internet Standard), RFC Editor, pp. 1–55, available at URL:https://www:rfc-editor:org/rfc/rfc1035:txt
5. J. Bushart and C. Rossow (2019) "Padding ain't enough: Assessing the privacy guarantees of encrypted dns," arXiv preprint arXiv:1907.01317.
6. Т.І. Коробейнікова, Т. Б. Федчук (2024) Огляд питання безпечного доступу до ресурсів системи доменних імен. Інформаційні технології та комп`ютерна інженерія, № 59(1), с. 40-53.
7. Коробейнікова Т.І., Федчук Т. Б. (Вересень 2023) Інформаційна технологія безпечного доступу до ресурсів DNS на базі ML-тренованих моделей ідентифікації трафіку. International periodical scientific journal «SWorldJournal», № 21 (part 1), с. 80–91. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-21-01.
8. Abu Al-Haija, Q.; Alohaly,M.; Odeh, A. (2023) A Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach. Sensors, 23, 3489, available at URL: https://doi.org/10.3390/s23073489
9. Abu Al-Haija, Q.; Al-Badawi, A. (2021) Attack-Aware IoT Network Traffic Routing Leveraging Ensemble Learning. Sensors, 22, 241.
10. Singh, S.K.; Roy, P.K. (December, 2020) Detecting malicious dns over https traffic using machine learning. In Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 20–21, pp. 1–6.
11. Wazen M. Shbair, Thibault Cholez, Antoine Goichot, and Isabelle Chrisment (2015) Efficiently bypassing SNI-based HTTPS filtering, IFIP.
12. Hynek, Karel & Vekshin, Dmitrii & Luxemburk, Jan & Cejka, Tomas & Wasicek, Armin (2022) Summary of DNS over HTTPS Abuse. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3175497.
13. Abu Al-Haija, Q.; Al-Badawi, A. (2021) Attack-Aware IoT Network Traffic Routing Leveraging Ensemble Learning. Sensors, 22, 241.
14. IETF (2015) RFC 7469: Public Key Pinning Extension for HTTP.
15. Mozilla. (August, 2024) MDN web docs - HTTP logging. available at URL: https://developer.mozilla.org/en-US/docs/Mozilla/Debugging/HTTP_logging
16. The Zeek Network Security Monitor (August 21, 2024) available at URL: https://zeek.org
17. Salesforce. GitHub: JA3 - A method for profiling SSL (August 21, 2024) available at URL: https://github.com/salesforce/ja3
18. Active Countermeasures. GitHub: RITA (Real Intelligence Threat Analytics) (August 19, 2024) available at URL: https://github/activecm/rita
19. IETF (2011) RFC 6066: Transport Layer Security (TLS), available at URL: Extensions: Extension Definitions.
20. GitHub: DNS over HTTPS – curl (August 21, 2024) https://github/curl/curl/wiki/DNS-over-HTTPS
21. IETF (2019) Issues and Requirements for SNI Encryption in TLS, draft-ietf-tls-sniencryption-09.
22. Lyu, M.; Gharakheili, H.H.; Sivaraman, V. (2022) A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques, ACM Comput. Surv, 55, 1–28.
23. Schapire, R.E. Explaining AdaBoost. In Empirical Inference; Schölkopf, B., Luo, Z., Vovk, V., Eds. (2013) Springer: Berlin/Heidelberg, Germany, pp. 37–52.
24. Arafat, M.Y. Hoque, S. Farid, D.M., Cluster-based under-sampling with random forest for multi-class imbalanced classification (2017) International Conference on Software, Knowledge, Information Management and Applications (SKIMA), Malabe, Sri Lanka, pp. 1–6.
25. Azeroual (2020) O. DataWrangling in Database Systems: Purging of Dirty Data, 5, 50.

References

1. T.I. Korobeinikova, S.M. Zakharchenko (2021) Tekhnolohii zakhystu lokalnykh merezh na osnovi obladnannia CISCO: navch. Posibnyk – Lviv, Vydavnytstvo Lvivskoi politekhniky, 188 s.
2. T.I. Korobeinikova, S.M. Zakharchenko. (2022) Kompiuterni merezhi: navch. Posibnyk – Lviv, Vydavnytstvo Lvivskoi politekhniky, 228 s.
3. P. E. Hoffman and P. McManus, Oct. (2018) DNS Queries over HTTPS (DoH), RFC 8484, Tech. Rep. 8484.
4. P. Mockapetris, Domain names - implementation and specification, RFC 1035 (Internet Standard), RFC Editor, pp. 1–55, available at URL:https://www:rfc-editor:org/rfc/rfc1035:txt
5. J. Bushart and C. Rossow (2019) "Padding aint enough: Assessing the privacy guarantees of encrypted dns," arXiv preprint arXiv:1907.01317.

6. T.I. Korobeinikova, T. B. Fedchuk (2024) Ohliad pytannia bezpechnoho dostupu do resursiv systemy domennykh imen. Informatsiini tekhnolohii ta komp`iuterna inzheneriia, № 59(1), s. 40-53.

7. Korobeinikova T.I., Fedchuk T. B. (Veresen 2023) Informatsiina tekhnolohiia bezpechnoho dostupu do resursiv DNS na bazi ML-trenovanykh modelei identyfikatsii trafiku. International periodical scientific journal «SWorldJournal», № 21 (part 1), s. 80–91. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-21-01.

8. Abu Al-Haija, Q.; Alohaly,M.; Odeh, A. (2023) A Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach. Sensors, 23, 3489, available at URL: https://doi.org/10.3390/s23073489

9. Abu Al-Haija, Q.; Al-Badawi, A. (2021) Attack-Aware IoT Network Traffic Routing Leveraging Ensemble Learning. Sensors, 22, 241.

10. Singh, S.K.; Roy, P.K. (December, 2020) Detecting malicious dns over https traffic using machine learning. In Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 20–21, pp. 1–6.

11. Wazen M. Shbair, Thibault Cholez, Antoine Goichot, and Isabelle Chrisment (2015) Efficiently bypassing SNI-based HTTPS filtering, IFIP.

12. Hynek, Karel & Vekshin, Dmitrii & Luxemburk, Jan & Cejka, Tomas & Wasicek, Armin (2022) Summary of DNS over HTTPS Abuse. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3175497.

13. Abu Al-Haija, Q.; Al-Badawi, A. (2021) Attack-Aware IoT Network Traffic Routing Leveraging Ensemble Learning. Sensors, 22, 241.

14. IETF (2015) RFC 7469: Public Key Pinning Extension for HTTP.

15. Mozilla. (August, 2024) MDN web docs - HTTP logging. available at URL: https://developer.mozilla.org/en-US/docs/Mozilla/Debugging/HTTP_logging

16. The Zeek Network Security Monitor (August 21, 2024) available at URL: https://zeek.org

17. Salesforce. GitHub: JA3 - A method for profiling SSL (August 21, 2024) available at URL: https://github.com/salesforce/ja3

18. Active Countermeasures. GitHub: RITA (Real Intelligence Threat Analytics) (August 19, 2024) available at URL: https://github/activecm/rita

19. IETF (2011) RFC 6066: Transport Layer Security (TLS), available at URL: Extensions: Extension Definitions.

20. GitHub: DNS over HTTPS – curl (August 21, 2024) https://github/curl/curl/wiki/DNS-over-HTTPS

21. IETF (2019) Issues and Requirements for SNI Encryption in TLS, draft-ietf-tls-sniencryption-09.

22. Lyu, M.; Gharakheili, H.H.; Sivaraman, V. (2022) A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques, ACM Comput. Surv, 55, 1–28.

23. Schapire, R.E. Explaining AdaBoost. In Empirical Inference; Schölkopf, B., Luo, Z., Vovk, V., Eds. (2013) Springer: Berlin/Heidelberg, Germany, pp. 37–52.

24. Arafat, M.Y. Hoque, S. Farid, D.M., Cluster-based under-sampling with random forest for multi-class imbalanced classification (2017) International Conference on Software, Knowledge, Information Management and Applications (SKIMA), Malabe, Sri Lanka, pp. 1–6.

25. Azeroual (2020) O. DataWrangling in Database Systems: Purging of Dirty Data, 5, 50.